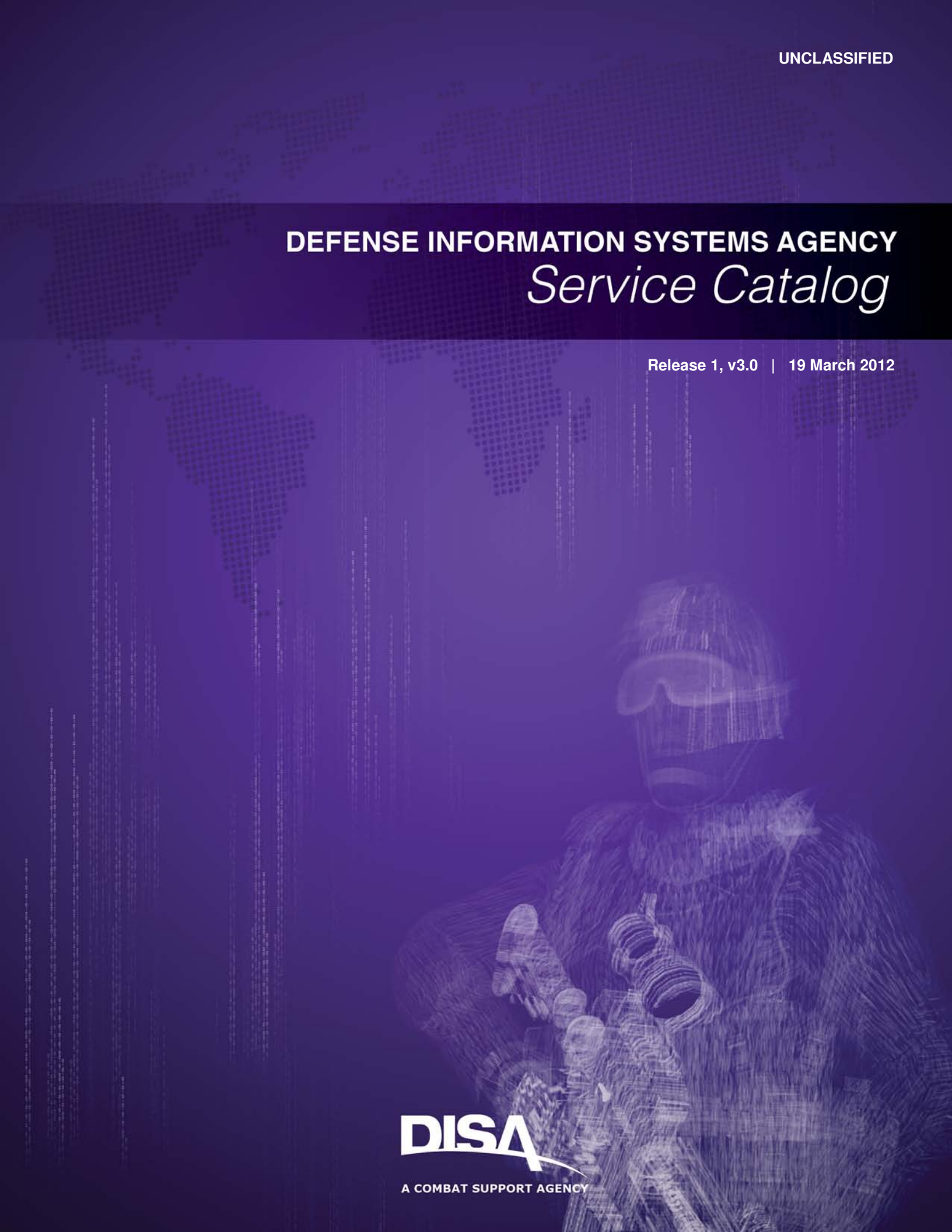
UNCLASSIFIED

DEFENSE INFORMATION SYSTEMS AGENCY
Service Catalog

Release 1, v3.0 | 19 March 2012



DISA

A COMBAT SUPPORT AGENCY

This page intentionally left blank.

Table of Contents

Campaign Plan – Service Key

- DISA Campaign Plan Line of Operation: Enterprise Infrastructure
- DISA Campaign Plan Line of Operation: Command & Control and Information Sharing
- DISA Campaign Plan Line of Operation: Operate and Assure
- DISA Campaign Plan Joint Enabler: Contracting
- DISA Campaign Plan Joint Enabler: Engineering
- DISA Campaign Plan Joint Enabler: Spectrum
- DISA Campaign Plan Joint Enabler: Testing

1 Introduction

The Defense Information Systems Agency (DISA) has published a Campaign Plan which framed our Lines of Operation and Joint Enablers, defined our strategic objectives, established initiatives, and allowed DISA to better align resources. The Campaign Plan allowed DISA to move from the traditional stovepipes which aligned services and operations along organizational lines into a coherent, integrated and seamless set of capabilities. This Service Catalog realigns the services we provide to our Mission Partners into that same new alignment.

1.1 Purpose

The purpose of the Service Catalog is to present our mission partners with a centralized resource of accurate information detailing current and/or emerging services DISA offers in the context of the Lines of Operation and Joint Enablers presented in the Campaign Plan. The Lines of Operation and Joint Enablers are:

DISA Campaign Plan Line of Operation: Enterprise Infrastructure

- The Enterprise Infrastructure Line of Operation unifies our communications, computing, enterprise, information assurance and network operations and services into a new "warfighting platform". The platform presents a versatile and protected environment where applications are developed and made available to our warfighters. The enterprise infrastructure allows the warfighter with appropriate credentials to access the network regardless of location or unit affiliation, thereby increasing productivity and flexibility.

DISA Campaign Plan Line of Operation: Command & Control and Information Sharing

- The Command & Control and Information Sharing Line of Operation encompasses the ability of a commander or decision maker to exercise authority and direction over assigned and attached forces and resources in the accomplishment of the mission. C2 is a critical capability as the fundamental enabler of joint services, which is the ability of multiple different military services to interoperate and provide combined arms capability that results in a force-multiplying effect during military operations. Information sharing refers to the ability of commanders to rapidly and effectively provide information to and consume information from mission partners, including coalition, operating across the strategic, operational, and tactical continuum.

DISA Campaign Plan Line of Operation: Operate and Assure

- The Operate and Assure Line of Operation allows DISA to provide a reliable, available, secure, and protected global net-centric enterprise in direct support to joint warfighters, national-level leaders, and other mission and coalition partners across the full spectrum of operations.

- Acquisition is the Joint Enabler that includes the processes and governance that enables DISA to develop and field new joint capabilities and services supporting the Lines of Operation, other Joint Enablers, and DoD as a whole.

DISA Campaign Plan Joint Enabler: Contracting

- The Contracting Joint Enabler provides DISA and our Mission Partners with the processes, disciplines and governance that enable the procurement of capabilities and services.

DISA Campaign Plan Joint Enabler: Engineering

- Engineering as a Joint Enabler provides DISA and our Mission Partners with the processes, disciplines and governance that enable innovation, design, development, and integration of capabilities, services, and standards to include enterprise-wide systems engineering.

- The Joint Enabler Information, Knowledge Management and Process Improvement provides DISA the means to enable effective service delivery, business systems and knowledge frameworks in the support of our Mission Partners.

- Support of our People is a key Joint Enabler allowing DISA to successfully recruit, train, educate, develop and sustain the DISA workforce.

- Planning is a Joint Enabler which allows DISA to set the course for the Agency over the short and long-term and to ensure resource availability to execute the Agency's vision and mission in support of our Mission Partners.

- The Joint Enabler Resources enables the planning, execution and financial stewardship of the DISA's financial resources.

DISA Campaign Plan Joint Enabler: Spectrum

- Spectrum as a Joint Enabler allows DISA and our Mission Partners to plan, manage, and engineer solutions for the electromagnetic spectrum used by DoD.

DISA Campaign Plan Joint Enabler: Testing

- Testing is the Joint Enabler that enables DISA and our Mission Partners to plan, conduct and manage interoperability testing and certification for DoD as well as the information assurance testing and certification for our Mission partners, DISA and DoD.

1.2 Scope

The scope of this catalog includes all DISA service offerings which can be made available to our Mission Partners and still be included in an informational catalog that is also available to the general public on the Internet. As service offerings are expanded and modified the Service Catalog will be quickly updated to ensure that the latest and most accurate service information is always available. DISA continues to research, design and deploy new service offerings to bring more efficient, effective and faster service to the warfighters and to the Department of Defense (DoD). The current initiatives in development are included in this catalog under the title "Pipeline Services". Finally, we include a full but condensed listing of the multiple offices, web sites and people that can assist you in obtaining and using these services.

2 Command and Control

Command and Control (C2) systems enable information superiority on the battlefield. They provide the commander with the information to make effective decisions, and they provide the warfighter the capability to access the information necessary to complete their mission.

2.1 Global Combat Support System – Joint (GCSS-Joint)

The Global Combat Support System – Joint (GCSS-J) provides the warfighter with a single, end-to-end capability to manage and monitor personnel and equipment through the mobilization process.
Global Combat Support System - Joint (GCSS-J), the Logistics' System of Record, provides a Joint Logistics Common Operational Picture (JLogCOP), ensuring the right personnel, equipment, supplies, and support are in the right place, at the right time, and in the right quantities across the full spectrum of military operations.

❖ Standard Features

- **Any Box** – the ability for end users to access GCSS-J capabilities via a web-browser. The primary browsers supported are Microsoft Internet Explorer and Mozilla Firefox.
- **Any User** – ability to access GCSS-J capabilities by anyone who has been given specific access privileges.
- **One Net** – the availability of essential logistics warfighter functions from a single network and workstation with single sign-on (SSO) to all applications.
- **One Picture** – the capability to integrate logistics information across all functional areas.
- **Quality Data** – refers to global, near real-time, accurate, integrated information provided through a robust and reliable communications infrastructure.
- **Anywhere** – refers to the ability of end-users to access the GCSS (CC/JTF) capabilities from any geographic location, where they have connectivity to the appropriate network.

❖ Optional Features

Tools and Joint Capability Areas based on authoritative data sources.

- Tools
  - Mapping - provides users a joint common operation picture
  - Reporting Tool – a web-based reporting application using authoritative data sources
- Joint Capability Areas
  - Deployment and Distribution
    - Create air and sea Nodes/Hubs using authoritative and user supplied data
    - Obtain seaport workload and ship container information via a map
    - Access to military and commercial trucks via real time data
  - Supply
    - Supported by WatchBoards and Logistics Analysis Tool; examples include
    - Tanker Deliveries
    - Unit Equipment
    - War Reserves
    - Munitions Inventory
  - Engineering
    - Joint Engineer Planning and Execution System - supports deliberate and crisis action planning
  - Planning
    - Supported by the Report Tool; examples include
    - Air Tracker

- OPLAN Analysis
- Readiness for Units in OPLAN
- Unit Move – Passenger Details

❖ **Value to Our Mission Partners**

GCSS-J is a software-intensive system designed to support the logistics needs of the joint community, providing interoperability, facilitating integration, and promoting data sharing across the spectrum of logistics. It provides end-to-end visibility of retail and unit level combat support capability up through national strategic level, facilitating information interoperability across and between combat support and C2 functions. GCSS-J provides the information technology capabilities required to move and sustain joint forces throughout the spectrum of military operations.

❖ **Rates/Pricing Information**

Cost of this service is covered by DISA with no charge to the end user.

❖ **Additional Information**

Additional information can be found at the GCSS-J website at:
http://www.disa.mil/Services/Command-and-Control/GCSS-J

❖ **How to Order**

Visit https://ca.intranet.disa.mil/gcssj/request_account.html to request an account. You have the option to request SIPRNet and NIPRNet accounts.

2.2 Global Command & Control System - Joint (GCCS-Joint)

The Global Command & Control System – Joint (GCCS-J) service offers vital connectivity to systems used to plan, execute and manage military operations for both joint and multinational operations. GCCS-J fuses select C2 capabilities into a comprehensive, interoperable system by exchanging imagery, intelligence, status of forces, and planning information. GCCS-J is focused on meeting emerging operational needs through sustainment and synchronization support to operational baselines (Global, COP I3 and JOPES) and subject matter experts to assist with critical operation and the GCCS-J Family of Systems (FoS).

❖ **Value to Our Mission Partners**

GCCS-J is a Command, Control, Communications, Computer, and Intelligence (C4I) system for achieving full spectrum dominance, consisting of hardware, software, procedures, standards, and interfaces that provide a robust, seamless C2 capability to the Commander-in-Chief (CINC), Secretary of Defense (SECDEF), National Military Command Center (NMCC), Combatant Commanders (CDRs), Joint Force Commanders, and Service Component Commanders. It is a suite of mission applications fusing select C2 capabilities into a comprehensive, interoperable system by exchanging imagery, intelligence, status of forces, and planning information. GCCS-J is the principal foundation for dominant battlespace awareness, providing an integrated, near real-time picture of the battlespace necessary to conduct joint and multinational operations. It offers vital connectivity to the systems the joint warfighter uses to plan, execute, and manage military operations.

The GCCS-J modernization vision is focused on continuing to decompose applicable existing applications into services, limiting local deployment, and continuing to expose data and scale services to support an enterprise implementation; reducing overall sustainment cost through use of more cost effective and appropriate COTS and HW products; and increasing the use of agile development practices.

2.3 Global Baseline-Situational Awareness (SA)

❖ **Standard Features**

Presents an integrated near real-time picture of the battle space for executing military operations, and includes:

- Red and Blue Force Picture
- CBRN (JEM / JWARN)
- Theater Missile Warning
- Alerts
- Air Tasking Exchange

❖ **Optional Features**

N/A

❖ **Rates/Pricing Information**

Charges to the end user will be on cost reimbursement basis with the costs being determined by the level of services provided.

❖ **Value to Our Mission Partners**

GCCS-J has accomplished over 1000 GCCS-J Component deployments for our Mission Partners at 53 critical sites.

❖ **For additional information on GCCS-J and how to order services:**

Please visit our DKO site at: https://www.us.army.mil/suite/designer

2.4 Joint Operation Planning & Execution System (JOPES)

Provides the joint warfighter with the ability to identify and source force requirements, validate sourced requirements, and request the time phased movement of forces to theater of interest in support of the joint force commander's needs. JOPES' suite of tools support the overarching policies and procedures that permit senior level decision makers and their staffs to analyze, plan, execute, and monitor military operations.

❖ **Standard Features**

- Builds force modules
- Provides force visibility
- Reflects scheduling and movement
- Produces reports

❖ **Value to Our Mission Partners**

JOPES is an integrated joint command and control system used to support military operation monitoring, planning, and execution activities. JOPES incorporates policies, procedures, personnel, and facilities by interfacing with Automated Data Processing (ADP) systems, reporting systems, and underlying GCCS-J ADP support to provide senior-level decision makers and their staffs with enhanced capability to plan and conduct joint military operations. The JOPES procedures and ADP systems are the mechanisms for submitting movement requirements to United States Transportation Command Joint operations and exercises. The JOPES latest version (v), JOPES v 4.2.1 Strategic Server Enclave (SSE), is an upgrade to the currently fielded GCCS-J JOPES v4.2.0.1 SSE.

❖ **Rates/Pricing Information**

Charges to the end user will be on cost reimbursement basis with the costs being determined by the level of services provided.

❖ **For additional information on GCCS-J and how to order services:**
Please visit our DKO site at: https://www.us.army.mil/suite/designer

2.5 Global Baseline-Integrated Imagery and Intelligence (I3)

Integrated Intelligence and Imagery (I3) provides intelligence support to the Common Operating Picture (COP) using an integrated suite of tools and services.

❖ **Standard Features**
- LIVE Predator UAV streaming
- Simultaneous search capability
- Imagery association to Military Intelligence Board (MIDB)
- Imagery plot to COP
- Analyst Workshop
- Still and motion imagery tools
- Joint Targeting Toolbox (JTT)
- Joint Threat Analysis Tool (JTAT)

❖ **Rates/Pricing Information**
Charges to the end user will be on cost reimbursement basis with the costs being determined by the level of services provided.

❖ **Value to Our Mission Partners**
GCCS-J has accomplished over 1000 GCCS-J Component deployments for our Mission Partners at 53 critical sites.

❖ **For additional information on GCCS-J and how to order services:**
Please visit our DKO site at: https://www.us.army.mil/suite/designer

2.6 GCCS-J-Initiatives: Cross Domain Solutions (CDS)

Provides cross domain data synch for GCCS-J data: COP (i.e. track data), structured intelligence, and imagery.

❖ **Standard Features**
- Improves the quality and consistency of GCCS-J COP and I3 data flows and interoperability between SCI, Collateral, & Coalition networks.
- Provides robust services for web-enabled COP and Intel support
- Achieves hardware and system administration efficiencies to reduce the number of guards and cloned systems currently deployed to share GCCS-J data
- Deploys Initial Operating capability (IOC) to DoD Intelligence Information System (DoDIIS) SE CONUS RSC in support of USCENTCOM
- Sustains interoperability with GCCS-J FoS and follow-on capabilities

❖ **Value to Our Mission Partners**
- Improve timeliness and relevance of actionable intelligence and decision support provided to JTF, Theater, and Tactical Commanders
- Reduce complexity of delivering GCCS-J managed content, applications, and services across security domains
- Streamline workflow and improve user experience in operating across several security domains

- CDS enables Combatant Commands/Services/Agencies (CC/S/A) with cross-domain communications for mission support without compromising the security of either information domain. High assurance guard systems have been employed to bridge the disparate information domains, filtering data based on policies and supporting bidirectional or unidirectional data flows. CDS capabilities aim to offer the most needed demands of the cross domain community by providing net-centric, service oriented, cross domain information sharing solutions with guaranteed quality of service for authorized users anywhere on the Global Information Grid. CDS is currently poised to achieve IOC of NIPR-SIPR Email at the beginning of calendar year 2012. This will be the first truly operational NIPR-SIPR Email and will incorporate lessons learned, increased functionality, greater security scrutiny, and ease of use. By mid-year 2012, CDS will have expanded capability to include bi-directional attachment sending with emails (SIPR-BICES Email) verses sending text only email.

❖ **Rates/Pricing Information**
Charges to the end user will be on cost reimbursement basis with the costs being determined by the level of services provided.

❖ **For additional information on GCCS-J and how to order services:**
Please visit our DKO site at: https://www.us.army.mil/suite/designer

2.7 GCCS-J-Initiatives: Enterprise Common Operating Picture (ECOP)

- Enterprise deployment of GCCS-J Situational Awareness components
- Expands COP user base and accessibility by establishing an enterprise accessible Common Operational Picture that allows authorized users to visualize COP data from any location on GIG using a web browser or agile client.

❖ **Standard Features**
- Expands on FY11 Unclassified COP activities to include the Global COP use case.
- Consolidates web and rich client visualization tools and implements an enterprise identity management solution for access control.
- Enhances remote data/service management capabilities.

❖ **Value to Our Mission Partners**
- Provides increased availability to Global COP data to the warfighter.
- Provides verified remote data/service management capability and processes to the warfighter.

❖ **Rates/Pricing Information**
Charges to the end user will be on cost reimbursement basis with the costs being determined by the level of services provided.

❖ **For additional information on GCCS-J and how to order services:**
Please visit our DKO site at: https://www.us.army.mil/suite/designer

2.8 GCCS-J-Initiatives: Joint C2 Common User Interface (JC2CUI)

Common User interface allows for single entry point for the warfighter to access C2 capabilities via the world wide web. User configurable thin client framework based on Ozone Widgets.

❖ **Standard Features**
- Builds and deploys a web client environment called the Joint C2 Common User Interface for single access point to disparate C2 web applications

- Provides a Widget-based framework on NIPR and SIPR
- Based on the NSA developed Ozone Widget Framework
- Integrates single sign-on solution for identification management
- Provides a base library of "widgets" (Core and C2 specific)
- Provides a Marketplace for the discovery and deployment of capabilities (widgets) – based on Ozone Market Place (OMP)
- Encourages broad participation from C/S/As for contribution and use

❖ **Value to Our Mission Partners**

- Due to seamless interface to capabilities JCUI simplifies training and increases the utility of the system due to reduction in different tools
- Significant increase to the ease of use of current highly capable but complex GCCS and other POR client applications
- Lightweight single purpose web applications based on the same data and functionality of GCCS (for users who don't need full GCCS Client functionality)
- Allows users to organize and define their own C2 Application desktop and profiles
- Greatly reduces time to field capabilities as web applications (widgets)
- Access to a growing Marketplace of widget based capabilities on the Enterprise (in the cloud)

❖ **Rates/Pricing Information**

Charges to the end user are determined by the level of services provided.

❖ **How to Order**

For additional information on GCCS-J and how to order services:

Please visit our DKO site at: https://www.us.army.mil/suite/designer

2.9 GCCS-J-Initiatives: Agile Client

Agile Client is a lightweight client workstation that provides a three-dimensional modeling cartographic engine.

❖ **Standard Features**

- Continues improvements to extensible open source framework (Java NetBeans).
- Improve distributed caching capability to better support DIL.
- Expand third party development model supported via plug-ins.
- Software development kit / Plug-in development toolkit.
- Developer workshops.
- Deploy Agile Client plug-in marketplace and update center for network provisioning of framework/plug-in updates.
- Establish Joint C2 governance process for plug-in marketplace.

❖ **Rates/Pricing Information**

Charges to the end user are determined by the level of services provided.

❖ **Additional Information-Value to Warfighter**

- Provides full mission capability in disconnected operation or degraded communication environments to the warfighter.
- Uses the NASA Work Wind mapping engine, which fully supports all NGA map types while providing expansion capability by using "NetBeans".

❖ **How to Order**

For additional information on GCCS-J and how to order services:

Please visit our DKO site at: https://www.us.army.mil/suite/designer

2.10 Joint Planning and Execution Services (JPES)

The Joint Planning and Execution Services (JPES) (formerly Adaptive Planning & Execution [APEX]) is the DoD's system that supports the policies, processes, procedures, and reporting structures needed to plan, execute, mobilize, deploy, employ, sustain, redeploy, and demobilize activities associated with Joint Operations. This service assists in the evaluation of processes and thus transforms the execution of Joint Operations.

❖ **Standard Features**

- **JPES Framework (JFW):** The JFW is composed of software "infrastructure" components that provide management, storage, and access to authoritative planning data. Data objects will be exposed through secure Simple Object Access Protocol (SOAP) based web services and synchronized with other planning databases as well as geographically distributed nodes. JFW will also include a separate business rules engine as well as a workflow manager in support of Adaptive Planning & Execution processes. A few of the core capabilities of JFW are:
  - **JPES Permission Manager (JPM):** Manages permissions for JOPES planning data and JPES data objects.
  - **Data Virtualization Layer (DVL):** Provides a high performance, in-memory federation of existing Authoritative Data Sources (ADS) exposed through secure SOAP based web services. JPES applications will be able to connect to the DVL to read from and write to disparate ADS.
  - **JPES Policy Decision Point (PDP):** Provides Attribute-Based Access Control (ABAC) through the use of a PDP which leverages Extensible Access Control Markup Language (XACML) Policy Store and Local attribute Store to make, permit, or deny access decisions on JPES resources.
- **Joint Force Protection (JFP):** The JFP System quickly retrieves and processes essential force projection information used to support decisions made by members of the Joint Planning and Execution Community (JPEC). A specific emphasis is placed on those processes that support identifying, requesting, sourcing, validating, scheduling, movement tracking, and closing of force capabilities requested by the supported commander. JFP provides visibility into execution of a plan by aggregating data from the following authoritative planning and execution sources such as:
  - Joint Operation Planning and Execution System (JOPES)
  - Global Status of Resources and Training System (GSORTS)
  - Global Transportation Network (GTN)
  - Joint Capabilities Requirements Manager (JCRM)
  - Automated Message Handling System (AMHS)
- **Joint Capabilities Requirements Manager (JCRM):** JCRM is a web-based software application that enables the Global Force Management (GFM) allocation process using a net-centric compliant architecture leveraging multiple authoritative data sources across the Department of Defense (DoD). JCRM was developed by the Global Force Management Continuous Process Improvement (GFM-CPI) effort under the direction of the Force Management Executive Committee (FMEC). It is the single software application for submitting and/or managing all force requirements (Emergent, Rotational, Exercise, Individual Augmentation and Contingency Planning) and is directed for use by all Combatant Commands (COCOM) and Services in the annual CJCS GFMAP PLANORD. GFM aligns force apportionment, assignment, and allocation in support of the National Defense Strategy (NDS), joint force availability requirements, and joint force assessments. It provides comprehensive insights into the global availability of U.S. military

forces/capabilities and provides senior decision makers a process to quickly and accurately assess the impact and risk of proposed changes in forces/capability assignment, apportionment, and allocation. There are seven components within JCRM. Each component, except for the System Administrator Module, provides necessary information and feeds to the next component to complete deployment orders and sourced forces for planned military operations. JCRM modules are:

- **The Requirements Module -** Captures "demand signal" on forces. The "demand signal" is the requirement to complete an individual, augmentee or team position to accomplish a planned military mission. These demands can be described as rotational or emergent, exercise, individual augmentee or contingency.
- **The Capabilities Module -** Consists of Operational Capability Packages (OCP), worksheets, also known as Request For Forces (RFFs), mapping Joint Capability Area (JCA) Universal Joint Task List (UJTL) to Unit Type Codes (UTC), and general searches for items such as relevancy, UTCs, Geolocations (GEOLOC), JCAs or UJTLs. OCPs provide the ability to generate packages of capabilities that include pertinent Global Force Management (GFM) and Joint Operation Planning and Execution System (JOPES) information, UTC via lookup/reference to Service Authoritative Data Sources (ADS) and Type Unit Characteristics File (TUCHA), GEO via lookup to GEOCODES; transform to initial JOPES Force Requirements Nominations (FRNs); transform to Requirements and RFFs; organizationally package OCPs in a hierarchical methodology; compare OCPs between COCOMs and users; and Reuse/copy "off-the-shelf" OCPs.
- **The Force Provider Module** - Utilizes nominations for the Force Provider or Joint Force Provider to create or modify force tracking number nominations, submit nominations to Joint Force Providers, accept or release Force Projection nominations, culminate in a Force Provider sourcing solution; building of **Joint Force Projection Orders** which allow for development of a Global Force Management Allocation Plan; and **COCOM Deployment Orders (DEPORDS)**
- **The Force Deployment Module** - Allows the communication of JCRM with JOPES via the JOPES Data Network Service (JDNETS) interface. This interface provides reconciliation of requested, ordered and deployed data, and creation of filters to validate FTNs ordered under GFM process with FTN in a JOPES Time Phased Force Deployment Data (TPFDD).
- **The Contingency Plans Module -** Supports the GFM process of capturing the "demand signal" for contingency planning requirements, and enhancing the contingency sourcing process through Force Provider visibility. It enables the user with proper roles and permissions to perform Contingency Sourcing, which supports the GFM and Adaptive Planning and Execution (APEX) planning continuum.
- **The Functional Manager Module** - Allows for the management of user accounts, roles and permissions, manages reference lists as a Functional Authority via Joint Requirement Code (JRCs)/Nomenclatures, Global Employment of Forces (GEF) Priorities, and Special Operations Command (SOCOM) Priorities. The Functional Manager Module also allows, with limited external interface configuration, United States Central Command (USCENTCOM) Functional Administrator to import data from Force Requirements Enhanced Database (FRED) and the United States Joint Forces Command (USJFCOM) Joint Staff Administrators to import data from Joint Training Information Management System (JTIMS) and Electronic Joint Manpower and Personnel System (eJMAPS).

- **The System Administrator Module** - Allows for a user with increased permissions to configure an external interface to modify Universal Resource Locator (URL) addresses, authenticate information, pull data from external sources; privileged functionality to cancel requirement change requests, and release object locks; manage reference lists; and view error logs.

Optional Features
N/A

Value to Our Mission Partners
JPES is a portfolio of capabilities that supports the contingency (deliberate), crisis action planning processes which rapidly transforms those joint operations plans into execution (movement) orders for the warfighters. Key elements of JPES include the JPES Framework (JFW) and Joint Force Projection (JFP).The JFW is a suite of software "infrastructure" components and services to support management, storage of, and access control to JPES data as web services enabled data objects as well as data distribution, synchronization, data business rule enforcement and workflow management in support of JPES capabilities. The JFP Portal provides a single, integrated force projection picture that links operators and logisticians at Service, Joint, and Agency levels using real-time, web-based, and network-centric information systems. The JCRM is a web-based GFM tool that increases the efficiency of the GFM process by providing senior DoD decision makers with a consolidated database of joint forces, capabilities, and requirements. JCRM will transition to DISA from JS J31 in the July 2012 timeframe.

JPES capabilities consist of support operations, helpdesk, software license renewals, software error correction, information assurance vulnerability alert (IAVA) compliance in the Secret, development, training, and COOP nodes. Future efforts are aimed at completing the enhancement of adaptive planning and execution capabilities.

Rates/Pricing Information
Cost of this service is covered by DISA with no charge to the end user.

Additional Information
N/A

How to Order

JPES POC	Contact Information
	Office: (301)225-5342 DSN: 375
	Office: (301)225-5267 DSN: 375

2.11 Multinational Information Sharing (MNIS)

The Multinational Information Sharing (MNIS) service serves to assist in the facilitation of information sharing among DoD components and eligible foreign nations in support of planning and execution of military operations.

❖ Standard Features

- CENTRIXS supports intelligence and classified operations information exchange and sharing up to SECRET Releasable (REL). CENTRIXS is federated among global and command enterprise environments. The global environment is managed by DISA to serve and interconnect command enterprise elements. The command enterprises consist of servers, applications, and encryption systems that form essentially autonomous service environments interconnecting command enclaves through existing regional communications networks for bilateral or multilateral access among cooperating nations and international organizations.
- CMNT (under construction - full menu coming January 2012)
- HARMONIEWeb (under construction - full menu coming January 2012)
- Pegasus/Griffin provides information sharing between participating nations for planning, implementing and executing multinational planning and operations. Information sharing capabilities requested by the Multinational Interoperability Council Principals through the Combined Communications-Electronics Board are provided between national SECRET level C2 systems of the participating nations. Services are provided by DISA at regionally located facilities. Current services include email with attachments, sharing (bi-directional) Common Operational Picture (COP), national reach back for liaison officers, directory service. Plans include web services, chat services and exchange of military messages.
- UISS-APAN (under construction - full menu coming January 2012)

❖ Value to Our Mission Partners

MNIS is a portfolio of initiatives to improve interoperability and information sharing with coalition partners. It provides standard community of interest services and applications to facilitate collaboration among DoD components and foreign nations. This functionality provides Cross Domain Service (CDS) that allows connectivity to national C2 systems and information sharing between multinational partners within an isolated sharing environment. Initiatives:

- **CENTRIXS** is the Combatant Commander's network for coalition warfighting. CENTRIXS is designed to be a global, interoperable, interconnected, inexpensive, and easy-to use system to share and exchange intelligence and operations information through reliable communications connectivity, data manipulation, and automated processes. The CENTRIXS environment is a combination of network and applications services. CENTRIXS provides a secured exchange of intelligence and operational information through reliable communication networks There are 40+ CENTRIXS networks/communities of interest (COIs) providing selected centralized services including: Active Directory/DNS Roots, VoIP, WSUS and Anti-Virus Definitions, and at least 80 countries plus NATO nations participate in the various CENTRIXS networks/COIs.
- **Pegasus/Griffin** is a multinational-developed, managed and resourced collection of networks and services that provides information sharing among their national classified (SECRET level) networks and C2 systems. Griffin enables participating nations to plan, implement and execute multinational planning and operations from the strategic to tactical headquarters level. It permits users to share SECRET REL information from their national C2 system workstations.
- **The Combined Federated Battle Laboratory Network (CFBLNet)** is a coalition RDT&E environment with Combined Communications-Electronics Board (CCEB) and the North Atlantic Treaty Organization (NATO) and other charter nations/organizations. CFBLNet leverages existing CCEB, NATO, and other national laboratories and test beds to support a wide range of coalition ISR experimentation and interoperability testing. As a combined environment and network, members have equal say in its use and management, yet specific initiatives may be configured among any number of participants. CFBLNet members respect sovereign and intellectual property rights of activities conducted on the network. CFBLNet is primarily a fee for service activity.

- **Unclassified Information Sharing** / **All Partners Access Network (UIS/APAN)**: A web 2.0 service that combines the benefits of unstructured collaboration (wikis, blogs, forums) and structured collaboration (file sharing, calendar) with the personalization of social networking. The existing functionality is maintained at USPACOM Pacific Warfighting Center (PWC). Through FY11 and FY12 it will sustain existing HARMONIEWeb COI User support, complete the standup and roll over of APAN users to UISC enterprise at DISA DECC-M, and expand functionality to all COCOMs and other mission partners. By Q3FY12 the goal is to stand up a shared enterprise service functionality - One Solution: Unclassified; Non-dot-mil; Gateway to DoD.

❖ Additional Information

Additional information can be found at the MNIS website at: http://www.disa.mil/Services/MNIS

❖ How to Order

Program Office: (301) 255-5536 / (301)255-5054

3 Computing

The world-class team of technicians in DISA delivers mature and standardized operations processes, centralized management, and partner-focused support. DISA manages all the partner data, including hardware components (computers, storage devices, and networks), software, and labor. DISA provides the stable environment within which our partners' applications can run.

3.1 Mainframe Hosting

DISA assumes responsibility for platform management by hosting DoD applications using DISA-provided hardware, operating systems (OSs) and labor.

3.1.1 UNISYS

DISA will host DoD Unisys applications using DISA-provided hardware, operating systems (OSs), and labor.

❖ **Standard Features**

- System Administration
- Security
- Data Communications
- Enterprise System Management (ESM) Software
- Level 2 Service Desk Support
- Storage
- Assured Computing/IT Service Continuity
- Mainframe Internet Access Portal (MIAP)
- Capacity Management

❖ **Optional Features**

Available upon request and will be charged directly to our partners in addition to any costs associated with rate-based services. Optional features include:

- Application Support
- Dedicated Logical Partition (LPAR)
- Dedicated Unisys Mainframe
- Classified COOP/Service Continuity

❖ **Rates/Pricing Information**

To see the DoD-approved rates for this service, please refer to:
http://www.disa.mil/Services/~/media/Files/DISA/Services/Computing/Rates.pdf

❖ **How to Order**

This service can be obtained by working with your Enterprise Services Directorate (ESD) Customer Management Executive (CME) team to complete a Service Request Form (SRF) that will identify the specifics of your requirement.

To obtain contact information for your CME team or the Service Level Management (SLM) hotline, please refer to the Points of Contact.

❖ **Additional Information**

DISA has standard performance level data available for our partners to view. Additional data can also be provided as requested. All performance data to be provided will be documented in the SLA which will be executed when the service is ordered.

Additional service and ordering information:

Organization	Contact Information
ESD Phone	CML: 303-224-1660 DSN: 926-1660
ESD Email	CSD_SLM@csd.disa.mil

3.1.2 IBM

DISA will host DoD IBM applications using DISA-provided hardware, operating systems and labor.

❖ **Standard Features**

- System Administration
- Security
- Data Communications
- Enterprise System Management (ESM) Software
- Level 2 Service Desk Support
- Storage
- Assured Computing/IT Service Continuity
- Mainframe Internet Access Portal (MIAP)
- Capacity Management

❖ **Optional Features**

The following features are available upon request and charged directly to the partner in addition to any costs associated with rate-based services. Optional features include:

- Application Support
- Dedicated Logical Partition (LPAR)
- Dedicated IBM Mainframe
- Classified COOP/Service Continuity

❖ **Rates/Pricing Information**

To see the DoD-approved rates for this service, please refer to:
http://www.disa.mil/Services/~/media/Files/DISA/Services/Computing/Rates.pdf

❖ **Additional Information**

DISA has standard performance level data available for our partners to view. Additional data can also be provided as requested. All performance data to be provided will be documented in the SLA which will be executed when the service is ordered.

❖ **How to Order**

This service can be obtained by working with your Enterprise Services Directorate (ESD) Customer Management Executive (CME) team to complete a Service Request Form (SRF) that will identify the specifics of your requirement.

To obtain contact information for your CME team or the Service Level Management (SLM) hotline, please refer to the Points of Contact. Additional service and ordering information:

Organization	Contact Information
ESD Phone	CML: 303-224-1660 DSN: 926-1660
ESD Email	CSD_SLM@csd.disa.mil

3.1.3 IBM Linux on System Z

Specialty engines on the Integrated Facility for Linux Mainframe allow the mainframe to run Linux workloads. What does this mean to our partners? ESD's Linux on System z environment offers many of the benefits of the traditional mainframe environment combined with the flexibility of Linux.

❖ **Standard Features**

- System Administration
- Security
- Data Communications
- ESM Software
- Level 2 Service Desk Support
- Storage
- Assured Computing/IT Service Continuity
- MIAP
- Capacity Management

❖ **Optional Features**

Because all our partners require different levels of support, ESD provides choices from the following supplemental features. Each feature has its own set of rates, priced per OE on the Linux on System z platform. However, if a partner has a uniquely large workload, ESD will work with the partner to develop an agreeable labor support cost method outside of these rates. Optional features include:

- Database Administration
- 24 x 7 System Administration
- 24 x 7 Database Administration
- 24 x 7 Application Support
- Local Operational Recovery

❖ **Rates/Pricing Information**

To see the DoD-approved rates for this service, please refer to:
http://www.disa.mil/Services/~/media/Files/DISA/Services/Computing/Rates.pdf

❖ Additional Information

DISA has standard performance level data available for our partners to view. Additional data can also be provided as requested. All performance data to be provided will be documented in the SLA which will be executed when the service is ordered.

❖ How to Order

This service can be obtained by working with your ESD Customer Management Executive (CME) team to complete a Service Request Form (SRF) that will identify the specifics of your requirement.

To obtain contact information for your CME team or the Service Level Management (SLM) hotline, please refer to the Points of Contact.
Additional service and ordering information:

Organization	Contact Information
ESD Phone	CML: 303-224-1660 DSN: 926-1660
ESD Email	CSD_SLM@csd.disa.mil

3.2 Server Hosting & Virtualization

The unit of measure for the basic Server service is the operating environment (OE), which DISA defines as an instance of an operating system (OS). One physical server could have one copy of the OS installed, in which case the OE is the server itself. However, one physical server could be carved into many partitions (similar to a mainframe), each of which has one copy of the OS installed. (These are called virtual OEs or virtual machines.) We charge Server rates at the OE level, not at the physical server level.

The OS (Windows, Linux or UNIX) and the number of sockets populated with central processing units (CPUs) will determine the size of the OE (Level 2 to 6). The rates differ based on size and OS. DISA will host DoD applications using DISA-provided hardware, operating systems and labor.

❖ Standard Features

- System Administration
- Security
- Level 2 Service Desk Support
- Maintenance costs for the monitoring software the Service Desk uses and costs associated with the DISA communications infrastructure

❖ Optional Features

Because each partner's processing requirements may differ from the next partner, ESD offers all our partners a selection of supplemental features. Each feature has its own set of rates, priced per OE, based on the size and type of OS. Optional features include:

- Hardware Services
- Application Support
- Web Administration
- Database Administration
- Oracle Database Software Maintenance

- 24 x 7 System Administration (SA)
- 24 x 7 Database Administration (DBA)
- 24 x 7 Application Support
- Cost-Reimbursable (Non-Rate) Services
- COOP/Service Continuity

❖ **Rates/Pricing Information**

To see the DoD-approved rates for this service, please refer to
http://www.disa.mil/Services/~/media/Files/DISA/Services/Computing/Rates.pdf

❖ **Additional Information**

DISA has standard performance level data available for our partners to view. Additional data can also be provided as requested. All performance data to be provided will be documented in the SLA which will be executed when the service is ordered.

❖ **How to Order**

This service can be obtained by working with your Enterprise Services Directorate (ESD) Customer Management Executive (CME) team to complete a Service Request Form (SRF) that will identify the specifics of your requirement.

To obtain contact information for your CME team or the Service Level Management (SLM) hotline, please refer to the Points of Contact.

Additional service and ordering information:

Organization	Contact Information
ESD Phone	CML: 303-224-1660 DSN: 926-1660
ESD Email	CSD_SLM@csd.disa.mil

3.2.1 Storage Support for Server-Based Applications

Our partners purchasing Server services are offered a wide array of storage opportunities that allow DISA to provide the level of service required to meet maximum acceptable data loss.

Rate-based server storage pricing is based on the gigabyte (GB) (raw) storage allocated per month and the level of service requested by the partner for data recovery, not application restoration based on Recovery Time Objective (RTO) and recovery Point Objective (RPO). Additional levels are cumulative, for example, R1 is (L1+R1) * GB storage.

The table below shows the options available for local recovery. The first entry is included as part of the L1 storage rate and is based on the use of locally available backup media, to recover on existing production storage capacity. Entries L2 and L3 are advanced local data recovery options.

❖ **Overview of Local Recovery options**

Level	Type	Description	Maximum Data Loss
L1	Default Local (Basic Service)	Recovery in place using production equipment and backup data	Seven (7) Days

Level	Type	Description	Maximum Data Loss
L2	Operational Local	Recovery in place using production equipment and backup data in a near-online state	24 Hours
L3	High-Availability (HA) Local	Recovery in place using production equipment and frequently updated backup data in a near-online state and/or designated remote site	8 Hours

NOTE: *Local recovery will not satisfy the Continuity of Operations (COOP)/Service Continuity requirements detailed in DoD Instruction 8500.2, which mandates a remote recovery strategy at a predetermined location. Operational recovery options will not, by themselves, satisfy the stated requirements for continuity.*

- **Standard Features**
  - Default Local Recovery (L1)

Overview of L1

Hardware	Depreciation and maintenance
	Infrastructure – switches, backup media
	Racks, cables
Software	Standard operating environment (SOE) and other storage resources
Labor	Storage administration
	Service Desk support
Backup Services	Standard weekly backup (one [1] copy onsite, retained four [4] weeks) designed for local recovery only.
	Incremental daily backup (one [1] copy onsite, retained two [2] weeks) designed for local recovery only.
	Standard weekly backup (one [1] copy offsite, retained four [4] weeks) designed for internal ESD recovery efforts only.
Data Center Services	Security
	Facilities
	Networks
	Tech refresh (storage array)
	Service Desk

❖ Optional Features

LocalRecovery, or "recovery in place," is a program designed to provide continuity in the event of an outage affecting the equipment, software and/or data that make up the application infrastructure but that leaves the primary facility operating and accessible. Based on the solutions selected, there are three advanced options for recovery.

- Operational Local/Operational Recovery Combination 1 (L2)
- High-Availability (HA) Local (L3)
- Cost Reimbursable Services

Options	Description	Maximum Data Loss
Local/Operational Recovery	Recovery in place using production equipment and backup data	7 Days
Advanced Local/Operational Recovery Combination 1	Recovery in place using production equipment and backup data in a near-online state	24 Hours
Advanced Local/Operational Recovery Combination 2	Recovery in place using production equipment and frequently updated backup data in a near-online state and/or designated remote site	8 Hours

NOTE: *DoDI 8500.2 requires recovery strategies to include a designated site for remote recovery efforts. Operational recovery options will not, by themselves, satisfy the stated requirements for continuity.*

❖ Rates/Pricing Information

To see the DoD-approved rates for this service, please refer to:
http://www.disa.mil/Services/~/media/Files/DISA/Services/Computing/Rates.pdf

❖ Additional Information

DISA has standard performance level data available for our partners to view. Additional data can also be provided as requested. All performance data to be provided will be documented in the SLA which will be executed when the service is ordered.

❖ How to Order

This service can be obtained by working with your Enterprise Services Directorate (ESD) Customer Management Executive (CME) team to complete a Service Request Form (SRF) that will identify the specifics of your requirement.

To obtain contact information for your CME team or the Service Level Management (SLM) hotline, please refer to the Points of Contact.

❖ Additional Information

Additional service and ordering information:

Organization	Contact Information
ESD Phone	CML: 303-224-1660 DSN: 926-1660

ESD Email	CSD_SLM@csd.disa.mil

3.2.2 Continuity of Operations (COOP)/Service Continuity for Server-Based Applications

DISA provides regulatory-compliant remote recovery capability, or Continuity of Operations (COOP), for our partners who purchase that service and document the requirement within their governing Service Level agreement (SLA). The standards and minimum requirements outlined in DoD Instruction (DoDI) 8500.2 include continuity-related Information Assurance (IA) controls. Those minimums form the foundation for the program as administered by DISA.

For mainframe processing, including IBM, Linux on System z *, and Unisys platforms, the cost of COOP/Service Continuity is included in the rates (*additional storage cost applies). For all server-based processing, the basic rates do not include this coverage. Our partners with server-based processing must "opt in" to the COOP program by specifically selecting and paying for the appropriate remote recovery protection. Standard storage solution programs used by DISA are designed to support internal DISA recovery efforts only.

It is DISA's policy that COOP will only be offered for those applications where DISA already has the production processing requirement. DISA will not pursue or accept "COOP Only" arrangements for processing.

- **Standard Features**

  COOP/Service Continuity consists of the policies, procedures, and programs that allow DISA, in concert with partner personnel, to provide an effective level of assurance that workloads will continue to process in accordance with regulatory requirements and documented obligations in SLAs. The continuity-related IA controls from DoDI 8500.2 are satisfied by the COOP program as overseen by ESD.

  For partners purchasing IBM and Unisys mainframe processing, there is an Assured Computing Environment (ACE) approach to providing COOP that will meet mission assurance category (MAC) II requirements (processor and data) for remote recovery. This approach is included in the standard rates for those services. For Linux on System z on the IBM mainframe, the rate includes the processing capacity and capability; however, an additional charge for the storage component of the recovery infrastructure is required.

  Server-based processing does not include COOP/Service Continuity in the basic rates and requires the partner to specifically select and pay for the desired and compliant coverage (see Optional Features).

- **Optional Features**

  There are six options available for server-based COOP/Service Continuity – five of these are standard options and one is an additional custom option.

  The table below shows the five standard options known as Remote Recovery Combinations (RRCs). In order to have a recovery option that meets the COOP requirements detailed in DoDI 8500.2, appropriate selections must be made for both storage (data) recovery and server (processor) recovery.

Option	MAC Level	Description	Storage Offering	Processor Offering	RTO/RPO
RRC 1	MAC III	Remote recovery using tape-based data backups and shared processing capability at the default designated recovery site	Basic Remote	Shared COOP	Recovery Time Objective (RTO) = 5 Days Recovery Point Objective (RPO) = 7 Days
RRC 1.2	MAC III	Remote recovery using replication of data and shared processing capability at the default designated recovery site	Operational Remote	Shared COOP	RTO = 5 Days RPO = 24 Hours
RRC 2	MAC II	Remote recovery using replication of data as well as a dedicated, pre-configured processing capability at the designated recovery site	Operational Remote	Dedicated COOP	RTO & RPO = 24 Hours
RRC 3	MAC II	Remote recovery using replication of data as well as a dedicated, pre-configured processing capability at the designated recovery site	High-Availability Remote	Dedicated COOP	RTO & RPO = 8 Hours
RRC 4	MAC I	Remote recovery using near-synchronous replication of data as well as dedicated, pre-configured, and operational processing capability at the designated recovery site	Non-Disruptive Remote (Host-Based Replication Only)	Dedicated COOP	RTO = 30 Min RPO = 1 Sec

Custom (Option 6) is available to those where mission requirements for a particular application, or suite of applications, are not adequately addressed by any of the standard options identified above.

- **Rates/Pricing Information**
  To see the DoD-approved rates for this service, please refer to:
  http://www.disa.mil/Services/~/media/Files/DISA/Services/Computing/Rates.pdf

- **Additional Information**
  DISA has standard performance level data available for our partners to view. Additional data can also be provided as requested. All performance data to be provided will be documented in the SLA which will be executed when the service is ordered.

- **How to Order**
  This service can be obtained by working with your ESD Customer Management Executive (CME) team to complete a Service Request Form (SRF) that will identify the specifics of your requirement. To obtain contact information for your CME team or the Service Level Management (SLM) hotline, please refer to the Points of Contact.

Service and ordering information:

Organization	Contact Information
ESD Phone	CML: 303-224-1660 DSN: 926-1660
ESD Email	CSD_SLM@csd.disa.mil

3.3 Application Monitoring

3.3.1 System Network Availability Performance System (SyNAPS)

SyNAPS will provide transaction performance monitoring. SyNAPS utilizes synthetic users to monitor both user and system initiated web traffic between client machines and servers throughout the world. SyNAPS will provide early warnings of availability and performance problems, help prioritize and accelerate problem resolution based on business impact, and ensure compliance with SLAs.

❖ **Standard Features**

- SyNAPS Probe Component. From a single management console, with the SyNAPS Probe component, SyNAPS will be able to potentially manage thousands of users' behavior and access points across multiple web-based applications. SyNAPS functionality will allow for user performance delivery monitoring in real-time and the utilization of enterprise applications to the warfighter.
- SyNAPS Client Monitor. As a SyNAPS data collector, the SyNAPS Client Monitor will proactively monitor enterprise applications in real-time, identifying application performance problems before users are aware a problem exists. The SyNAPS Client Monitor will enable the application owner to monitor sites from various locations and will be able to emulate the end-user's experience. This will allow the application owner to assess site performance from different client perspectives.
- SyNAPS Dashboard. The dashboard is a role-based, user-emulated, and customizable graphic user interface (GUI) that will provide a common environment combining real-time application stability and historical performance data for immediate review. SyNAPS partners will be able to create personalized reports from dozens of predefined templates, enabling the application owner to focus on the key performance indicators (KPIs)

❖ **Rates/Pricing Information**

To see the DoD-approved rates for this service, please refer to:
http://www.disa.mil/Services/~/media/Files/DISA/Services/Computing/Rates.pdf .

❖ **Additional Information**

DISA has standard performance level data available for our partners to view. Additional data can also be provided as requested. All performance data to be provided will be documented in the SLA which will be executed when the service is ordered.

❖ **How to Order**

This service can be obtained by working with your ESD Customer Management Executive (CME) team to complete a Service Request Form (SRF) that will identify the specifics of your requirement. To obtain contact information for your CME team or the Service Level Management (SLM) Hotline, please refer to the Points of Contact.

Additional service and ordering information:

Organization	Contact Information
ESD Phone	CML: 303-224-1660 DSN: 926-1660
ESD Email	CSD_SLM@csd.disa.mil

3.3.2 Computing Data Transmission

DISA has network monitoring tools at its disposal to provide service for our partners. DISA provides and maintains the GIG utilized by our partners. Network operations support is provided by a 24x7 staff responsible for identifying and resolving network problems, upgrading network devices and conducting change management. Non-classified Internet Protocol Routing Network (NIPRNet) and Secret Internet Protocol Network (SIPRNet) network availability is built into the system via hardware and circuit diversity throughout the Wide Area Network (WAN).

DISA is responsible for separate enclaves used to support Defense Enterprise Computing Center (DECC) connectivity and applications. The same degree of circuit and hardware redundancy is provided to support the same degree of survivability. DISA hosts DoD demilitarized zone (DMZ) access nodes and DoD DMZ extensions that provide our partners with the ability to secure their applications in accordance with the DoD DMZ Security Technical Implementation Guide (STIG).

❖ **Standard Features**

The communications component is comprised of the DISA internal communications infrastructure and support teams. This infrastructure allows end-users, anywhere in the world, to connect safely and securely to the data that resides within DISA's processing centers.

NOTE: *Partner-specific communications enclaves, community-of-interest networks, virtual private networks, etc., are cost-reimbursable and are not part of the ESD communications infrastructure.*

- Data Transmission Options
- DISA will provide a variety of options to satisfy data transmission requirements to mitigate the potential risk with using unauthorized ports and protocols. These services are no longer billed to the partner. The following table describes each of the options.

Traffic Flow	Solution to Use	Notes
Site-to-site Virtual Private Networks (VPNs)	Varies	
.com → .mil (DECC)	Business to Business (B2B)	Complete B2B/VPN checklist and follow instructions enclosed.
.mil → .mil (DECC)	Policy-Based Co-Location (PB Collo)	If partner is collocated at DMZ, use partner VPN equipment. If partner is not collocated at DMZ, use DISA provided VPN. Complete B2B/VPN checklist and follow instructions enclosed.
.mil (DECC) →.mil (DECC)	Inter-DECC Virtual Routing and Forwarding (VRF)	No configuration needed

Traffic Flow	Solution to Use	Notes
DISA has deployed proxies that are used for any .com or .mil → .mil (DECC) based on Ports, Protocols and Services Management (PPSM) and associated boundaries	DMZ Proxy	N/A
Ports 20,21 – File Transport Protocol (FTP) (User initiated)	Mainframe Internet Access Portal (MIAP)	Complete MIAP application online at https://miap.csd.disa.mil
Ports 20,21 – FTP (Batch initiated)	B2B or PB Collo & Global Exchange (GEX) (on the backside)	Complete B2B PB Collo checklist as well as the GEX checklist
Port 22 – Secure Shell (SSH)/Secure FTP (SFTP)	GEX	Complete GEX checklist
Port 23 – Telnet	MIAP	Complete MIAP application online at https://miap.csd.disa.mil
Port 25 – Email	Mail Relay Services	Complete Mail Relay checklist
Port 80 – Hypertext Transfer Protocol (HTTP)	Web Proxy	Complete Web DMZ checklist
Port 443 – HTTP Secure (HTTPS)/Secure Socket Layer (SSL)	Web Proxy	Complete Web DMZ checklist
Port 1414 – Message Queuing (MQ) Series	GEX	Complete GEX checklist
.mil (DECC) → .com or .mil on Transmission Control Protocol (TCP) port 80 or 443	DMZ Forward Proxy	No configuration needed above DMZ VPN Router (top side of the Community of Interest Network [COIN])
Any .mil → .mil (DECC) that is not proxiable or is not required to be proxied based on PPSM and associated boundaries	DMZ Non-Proxy	Firewall (FW) rules need amended in Non Proxy context on DMZ FW for required ports.

NOTE: To obtain any of the checklists referenced in the above table, please the Enterprise Services Directorate (ESD)

The following communication services are included in the basic processor rates and the partner will not incur an additional charge.

- B2B Gateway/DMZ Non-Proxy Gateway
- Web DMZ

❖ Rates/Pricing Information

These data transmission services are included in the application support rates and will not cause additional cost to the customer.

❖ Additional Information

DISA has standard performance level data available for our partners to view. Additional data can also be provided as requested. All performance data to be provided will be documented in the SLA which will be executed when the service is ordered.

❖ **How to Order**

Data Communications services can be obtained by working with your Enterprise Services Directorate (ESD) Customer Management Executive (CME) team to complete a Service Request Form (SRF) that will identify the specifics of your requirement.

To obtain contact information for your CME team or the Service Level Management (SLM) hotline, please refer to the Points of Contact.

Additional service and ordering information can be found by emailing or calling ESD.

Organization	Contact Information
ESD Phone	CML: 303-224-1660 DSN: 926-1660
ESD Email	CSD_SLM@csd.disa.mil

3.4 Web Hosting

DISA can provide three levels of Web Hosting, ranging from "simple" to "complex." The standard services are based on the use of Microsoft Windows Standard/Internet Information Services (IIS) or Linux/Apacheor Linux on System Z/Apache on DISA-provided hardware. Web Hosting service offerings include Mission Assurance Category (MAC) III remote recovery. The offerings are summarized as follows:

Bronze – Simple to intermediate-sized web sites, with DISA-supported scripting and small data requirements (less than one GB per site)

Silver – Intermediate-sized web sites requiring a dedicated OE or OEs, scripting support, and increased storage requirements (five GB of data per OE)

Gold – Intermediate-sized to complex web sites requiring a dedicated server, scripting support, and significant storage (20 GB of data)

NOTE: Restricted WEB authorized web sites (WEB-R) and unrestricted public web sites (WEB-U) are available through the standard rate structure.

❖ **Standard Features**

All Web Hosting Levels include the following features:

- Project Management
- Basic Services
- Systems Administration (SA)
- Hardware Services
- Information Assurance (IA)
- Facility Environmentals (Heating, Ventilating, and Air Conditioning [HVAC]; power; Uninterruptible Power Supply [UPS])

❖ **Optional Features**

Database as a Service (DaaS) is also available, but is currently offered on a very restricted basis, and is only available to those partners that have selected the Bronze or Silver level web hosting service. Using the DISA Capacity Services approach, the DaaS promotes improved server utilization and

reduces operational and environmental impacts created by dedicated servers. DaaS offers partners two OE choices:

- Microsoft Structured Query Language (SQL) Server
- MySQL

❖ Value to Our Mission Partners

DISA can provide three levels of the web hosting cloud service, ranging from "simple" to "complex." The standard services are based on the use of Microsoft Windows Standard/Internet Information Services (IIS) or Linux/Apache on DISA-provided hardware.

❖ Rates/Pricing Information

To see the DoD-approved rates for this service, please refer to:
http://www.disa.mil/Services/~/media/Files/DISA/Services/Computing/Rates.pdf

❖ Additional Information

DISA has standard performance level data available for our partners to view. Additional data can also be provided as requested. All performance data to be provided will be documented in the SLA which will be executed when the service is ordered.

❖ How to Order

This service can be obtained by working with your ESD CME team to complete a Service Request Form (SRF) that will identify the specifics of your requirement.

Coming Soon – Online Ordering!

To obtain contact information for your CME team or the Service Level Management (SLM) hotline, please refer to the Points of Contact. Additional service and ordering information:

Organization	Contact Information
ESD Phone	CML: 303-224-1660 DSN: 926-1660
ESD Email	SLM@csd.disa.mil

4 Contracting Services

Purchasing telecommunications and information technology (IT) products and services for the military is one of DISA's key roles within the Department of Defense (DoD).

Our contracting and procurement experts use a variety of contract vehicles to increase acquisition speed, reduce costs, and ensure the men and women of our armed services have the cutting-edge services and capabilities they need to fulfill their missions.

❖ Value to Our Mission Partners
- DISA provides Enterprise Acquisition Services (EAS) for purchasing telecommunications and information technology (IT) products and services from the worldwide commercial sector to meet Department of Defense (DoD) and authorized non-defense customers' needs. Services include acquisition planning, procurement, tariff surveillance, cost and price analyses, and contract administration. DISA is the mandated single source for procuring DoD long haul telecommunications requirements.
- DISA also establishes large contract vehicles available to DoD for essential IT services such as engineering, hardware, equipment and maintenance, integration and support, information security, computer technology, and Defense Information System Network (DISN) access. Non-DISN telecommunications circuits and systems are ordered on an individual basis and are fully reimbursed by customers. The EAS encompasses a variety of support services to meet DoD information technology contract requirements and provides contract support to all DISN subscription services. The EAS fee-for service remains at 2.00% for FY 2012.

For an overview of DISA contracting & procurement operations please go to the Defense Information Technology Contracting Organization web site at: https://www.ditco.disa.mil/

4.1 Online Resources for Government Buyers

4.1.1 DISA Contracts Guide

- For information on Indefinite Delivery/Indefinite Quantity (IDIQ) Contracts please go to:
- http://www.disa.mil/Services/Contracting/Contracts-Guide/Indefinite-Delivery-Indefinite-Quantity
- For information on Blanket Purchasing Agreements (BPA) please go to:
- http://www.disa.mil/Services/Contracting/Contracts-Guide/Blanket-Purchasing-Agreements
- For information on Basic Ordering Agreements (BOA) please go to: http://www.disa.mil/Services/Contracting/Contracts-Guide/Basic-Ordering-Agreements
- For additional Information: (301) 225-4120, DSN 375

4.1.2 DISA Direct Order Entry (DDOE)

DISA's ordering suite of tools for requesting Telecommunication Products and Services is DISA Direct, also referred to as DISA Direct Order Entry (DDOE). The DDOE portion of DISA Direct is the ordering tool. All persons requiring access to DISA Direct to place orders must create a Userid and then utilize the Registration tool to obtain the appropriate role for access to the various DISA Direct tools.

Our goal with DISA Direct is to provide our customers with one stop to gather information about the products and services offered by DISA, place orders to acquire these products/services, and perform life-cycle management of these assets.

For features, ordering information and additional information please go to;
https://www.disadirect.disa.mil/products/asp/welcome.asp

4.1.3 Wide Area Work Flow (WAWF)

A DoD system designed to automate the processing of payment documents in a "Paperless" Web-based environment.

- Standard Features
  WAWF electronically captures and coordinates four basic pieces of payment information:
  - Contract (Links to EDA)
  - Vendor invoice
  - Receiving Report
  - Payment Initiation with DFAS payment systems (A copy of the contract, invoice, and make payment)

- For Additional Information
  For Information regarding access and use please go to;
  http://www.ditco.disa.mil/hq/WAWF/home.asp

4.1.4 Telecommunication Inventory and Billing Information (TIBI)

TIBI is a DISA system designed to provide online access to integrated billing statements for DISA Telecommunication Services and Enterprise Acquisition S services. TIBI's primary stated objectives are to display billing information, background, and detail supporting the bill; and provide customers and managers with increased visibility of order data and associated metrics.

A DDOE account is required for TIBI access. The TIBI may be accessed at: https://www.ditco.disa.mil/ or https://www.disadirect.disa.mil/products/asp/welcome.asp.

4.2 Online Resources for Vendors

4.2.1 Contracting Opportunities

An online posting of current contracting opportunities with DISA can be found at:
https://www.ditco.disa.mil/dcop/Public/ASP/dcop.asp
http://www.ditco.disa.mil/hq/contracts/encorIIchar.asp

(This page also contains info about other DISA vehicles.)

Click **Task Ordering Guidelines**, and you will see this page:
http://www.ditco.disa.mil/hq/contracts/encorIIguide.asp

4.2.2 Office of Small Business Programs

The DISA Office of Small Business Programs (OSBP) advises the Director of DISA on small business matters, and represents the Agency before Congress, the Office Secretary of Defense (OSD), and other agencies in accordance with DFARS 19.201 (d)(2). It also participates and monitors the DISA acquisition process, and develops and monitors the disadvantaged business program to ensure that small business, women owned, small disadvantaged business concerns and Historically Black Colleges, Universities, and Minority Institutions (HBCU/MI's) receive a fair portion of DISA contract awards.

❖ **Functions**

- Promoting the use of small, small disadvantaged, small women owned, service-disabled veteran owned small business and historically black colleges/Universities and minority institutions.
- Advocating equitable treatment of small firms in support of subcontracting goals.
- Monitoring relevant legislation and information that may impact the DISA small business program in general, and soliciting customer feedback.
- Providing individualized technical assistance by conducting outreach programs, such as workshops, conferences, forums and maintaining client databases.

❖ **Additional Information**

For additional information please call (301) 225-6003, DSN 375 or email disasmallbusinessoffice@disa.mil.

4.2.3 Central Contractor Registration

Central Contractor Registration (CCR) is the official, FREE on-line registrant database for the U.S. Federal Government. CCR collects, validates, stores and disseminates data in support of agency acquisition and award missions. You do not need pay to register in CCR. Learn more about CCR Policy and Background.

❖ **To register and for additional information**

To register and to get additional information, please refer to: https://www.bpn.gov/ccr/

5 Enterprise Engineering

5.1 Engineering and Modeling

5.1.1 Joint Communication Simulation System

DISA develops and maintains the Joint Communication Simulation System (JCSS) for the Department of Defense. JCSS provides military planners and system analysts with a modeling and simulation (M&S) tool capable of modeling the performance characteristics of applications and networks. The primary advantage of JCSS is its extensive library of military models; including tactical radios, satellite networks, encryption devices, and others, many of which are provided by the JCSS user-community (SPAWAR, CERDEC, PEO-JTRS, etc.).

JCSS is used throughout a project's life cycle, from initial design concept to deployment and sustainment. During conceptualization, JCSS is used to optimize design parameters, quantify performance characteristics, and determine the scalability of the technology. Once a design is finalized, JCSS is used to model the new technology with the existing network infrastructure. After integration, JCSS can be used to plan for future enhancements by creating specific 'what-if' type scenarios. All of these advantages make JCSS a complete M&S solution.

- **Standard Features**
  - Extensive Commercial and Military Device Model Library
  - Template Organization and OPFAC Models
  - Device Configuration Information Import
  - Scenario Development
  - Capacity Planning
  - Terrain Modeling
  - Wireless Modeling
  - High Level Architecture Support
  - DoDAF Import/Export Support
  - Collaborative Planning

- **Optional Features**
  JCSS is based on a COTS tool, OPNET Modeler, allowing users access to commercial features licensed through OPNET. OPNET's website provides a complete list of optional features usable with JCSS (www.opnet.com).

- **Rates/Pricing Information**
  DISA provides JCSS to DoD civilians, military personnel, and contractors free of charge. JCSS is also available to coalition partners through foreign military sales, with cost dependent on number of licenses, training, and other specific requirements.

- **Additional Information**
  For more information about JCSS please visit our website at www.disa.mil/jcss

- **How to Order**
  Software requests are made through the JCSS website and support is offered by either phone or email:

For Further Information	
JCSS Website (General Info and Software requests)	www.disa.mil/jcss
JCSS Support Phone	CML: 301-225-7361 DSN: 375-7361
JCSS Support Email	JCSS@disa.mil

5.1.2 GIG Technical Guidance for Information Technology Standards

DISA develops, promulgates and maintains a catalog of information technology (IT) standards, standards profiles and interoperability compliance requirements to meet DISA product and service priorities as well as the needs of the Department of Defense (DoD), with emphasis on commercial and open systems standards. As the DoD Executive Agent for IT standards, the Enterprise Wide Systems Engineering (EWSE) supports standards-based end-to-end Interoperability assessments, technical guidance and evaluation to Joint programs.

The GIG Technical Guidance Federation (GTG-F) is a suite of software applications on the NIPRNet and SIPRNet (June 2012) that provides technical guidance across the Enterprise to achieve net-ready, interoperable, and supportable GIG systems. The GTG-F assists program managers, portfolio managers, engineers and others in answering two questions critical to any Information Technology (IT) or National Security Systems (NSS): (1) Where does the IT or NSS fit, as both a provider and consumer, into the GIG with regard to End-to-End technical performance, access to data and services, and interoperability; (2) What must an IT or NSS do to ensure technical interoperability with the GIG. The GTG-F content provides the technical information to various users in addressing and resolving technical issues needed to meet functional requirements (i.e., features and capabilities) of the GIG. This GTG-F content consists of and is based on GIG net-centric IT standards, associated profiles, engineering best practices and reference implementation specifications.

- **Standard Features**
  - GTG-F Configuration Management Board (Application Suite / Content)
  - Streamlined User Account Management via the PM Portal (PM-P)
  - Enhanced Information Support Plan (Enterprise Services Version)
  - GIG Technical Profiles (GTP)
  - Interoperability Assessment Module (IAM)
  - DoD Information Technology Standards Registry – Online (DISROnline)
  - Joint I&S Certification Document Repository of Legacy Programs (ISP / JCIDS)
  - CAC enabled / PKI controlled access
  - GTG/EWSE Content Collaboration WIKI
  - DoDAF Standards View Validation (StdV-1/2) Support

- **Optional Features**
  GTG-F is a reusable net-centric technology framework application with four modules for user registration, Information Support Plan development online, GIG Technical profile declaration; IT Standards profile development and data-centric analysis/assessment within one tool suite. Global Information Grid Technical Guidance Federation website provides an overview and access to the specific modules: https://gtg.csd.disa.mil/.
- **Rates/Pricing Information**
  DISA provides DoD civilians, military personnel, and contractors to support this Interoperability and Supportability mission with no charge to the end user.

❖ **Additional Information**
For more information about the Interface Standards Division, please visit our website at http://www.disa.mil/About/Our-Organization-Structure/EE/EE3

❖ **How to Order**
The GTG-F website and customer support is offered by either phone or email:

For Further Information	
GTG-F Website (General Info)	https://www.intelink.gov/wiki/Portal:GIG_Technical_Guidance/GTG-F_Systems_Documentation
GTG-F Support Phone	CML: 301-225-7400 DSN: 375-7400
GTG-F Support Email	EE3TechSupport@disa.mil

5.1.3 Interoperability Enhancement Process/iSmart (IEP/iSmart)

The interoperable Systems Management and Requirements Transformation (iSMART) process is an internationally accepted means to achieve visibility of interoperability challenges in the development of information systems and communications media, including tactical data links. It provides analysis of interoperability across operational and strategic data communications systems down to the tactical edge where the warfighter is located.

The iSMART process is a systems engineering approach to achieving interoperability in a cost-effective manner. It is the adoption of iSMART that 'provides an early insight to IO issues and an opportunity to cost effectively correct these before development commences.' This iSMART Handbook describes the elements of the iSMART process, the various products that can be achieved and the breadth of analysis which can take place. It shows the utility of iSMART during the development of a proposed system or its application in a fielded system of systems.

The strength of the iSMART process is the way separate elements can be used individually for small focused analysis or combined, synergistically, to provide a valuable analysis pertaining to the interoperability of the systems under consideration. iSMART is used internationally to support the achievement of effective interoperability at many levels. It is currently the IO process of choice in the US, UK, Australia, The Netherlands, Norway, Switzerland, and Sweden, amongst others. Its application can be tailored to particular national requirements/reference implementation specifications.

❖ **Standard Features**
- Interoperability Analysis and Management
- JTRS/SCA Data Links
- Net Management
- Gateways Range Extension
- Architectural (MODAF) Views
- IER Matrix Analysis
- Standards High-Level Link Requirements
- System of System Information Exchange Capability

❖ **Optional Features**
- Wide Area Network (WAN) Interoperability Testing

- Live Interoperability Testing
- Integration Testing

❖ Rates/Pricing Information

DISA provides DoD civilians, military personnel, and contractors to support this Interoperability and Supportability mission with no charge to the end user.

❖ Additional Information

For more information about the Interface Standards Division, please visit our website at http://www.disa.mil/About/Our-Organization-Structure/EE/EE3

❖ How to Order

The IEP/iSmart website and customer support is offered by either phone or email:

For Further Information	
IEP/iSmart Website (General Info)	https://www.us.army.mil/suite/group/23877
IEP/iSmart Support Phone	CML: 301-225-7400 DSN: 375-7400
IEP/iSmart Support Email	EE3TechSupport@disa.mil

6 Enterprise Services

6.1 Applications

6.1.1 Joint Enterprise Email (JEE)

Joint Enterprise E-mail (JEE) is a user-facing IT service intended for the DoD enterprise; it is a scalable and affordable alternative to each of the DoD components deploying and maintaining their own enterprise e-mail service. Adoption of the JEE service will necessarily consolidate e-mail infrastructure, centralize e-mail management, reduce the cost per user, and keep pace with industry functionality and innovation. JEE provides three fundamental capabilities:

- It is a messaging platform; users have the ability to exchange digitized correspondence, including attachments among themselves or with other e-mail systems using the network.
- It exists in the mail.mil domain and all users will have standard e-mail addresses with that domain name.
- It allows calendaring; JEE provides the ability to schedule and coordinate meetings with people and NPEs. Because this service is provided for the DoD enterprise, it allows calendaring across the DoD components.
- Some of the important characteristics of JEE are summarized in the table below:

Features or Attribute	Enterprise Email Service Characteristics
Global access; regional focus	Partner e-mail sites are globally accessible, but regionally focused. Users can log in from anywhere in the world.
Client Access Licenses (CALs)	Partners MUST have a standard CAL.
Availability	• Exchange: 99.9 percent • Outlook Web Access (OWA): 99.9 percent • Blackberry Enterprise Server (BES): 99.9 percent
Tier II Service Desk Support	A Tier II Service Desk will be provided by the Global Information Grid (GIG) Infrastructure Services Management Center (GISMC) for partners' Tier I and/or Tier II Service Desks; partners must operate their own Tier I Service Desk to coordinate with end users. A partner's Tier 1 may escalate issues to ESD's Tier II Service Desk when appropriate.
Scheduled Maintenance	Automated service interruptions (ASIs) • ASI coordinated with Partner's Service Desk • ASI impact application specific • Partner will have input into date/time of service interruption
Emergency Maintenance	Emergency maintenance will be approved by the Emergency Change Advisory Board (ECAB) and often have reduced or delayed testing. A partner's Service Desk will be informed through escalation process established prior to partner migration and documented in the concept of operations (CONOPs).
Authentication	The EASF will be used to authenticate users; Users MUST authenticate directly with the e-mail application with Transport Layer Security (TLS) & their CAC. Username and password will be made available for SIPRNet when available.

Features or Attribute	Enterprise Email Service Characteristics

Storage	• Business users (Outlook Anywhere) will receive a 4GB mailbox
	  ○ 512MB of 4GB will be online in Exchange
	  ○ E-mails will be automatically archived (no intervention from the user) once the mailbox reaches 512MB or the message is 45 days old, whichever occurs first.
	• OWA users will receive a 512MB mailbox
	  ○ E-mails will remain online in Exchange. There is no archiving for OWA-only users.
	• Users will be advised when they are getting close to reaching their limits.
	• Archive database will conduct incremental backups every night and a full backup once a week. Exchange servers will be backed up nightly

Content & Records Management (C&RM)	E-mail is NOT a DoDD 5015.2 certified records management platform; E-mail content should be considered to be unmanaged. A separate service for C&RM based on the IBM FileNet platform is being developed and will be integrated with the e-mail offering.
Third Party Software	The following third party software is included: • Systems Center Operations Manager (SCOM) • Threat Management Gateway (TMG) • Active Directory (AD) • Tivoli Provisioning Manager • Tivoli Monitoring • Tivoli Monitoring (Cap Mgt module) • Tivoli Enterprise Console • BladeLogic RSCD Agent v8.0 • DisKeeper 2010 Server Edition • McAfee VirusScan Enterprise • McAfee Agent (formerly Common Management Agent - CMA) • Mail Security for Exchange • ActivClient CAC • Tumbleweed VA Desktop Validator Enterprise • CommVault Simpana Data Archiver for E-mail (Backup/Archival software)

❖ Standard Features

- Accessibility via a browser interface through OWA
- Each user allotted a 512 MB sized mailbox
- Accessibility from the NIPRNet or virtual private network (VPN)
- Each service delivery location will include capacity and local redundancy, as well as a continuity of operations (COOP) site separated by a significant geographic distance.
- The DoD component Service Desks are the end-users' point of contact for any problems or requests related to the JEE service. ESD will provide a Tier II Service Desk to which DoD component Service Desks escalate issues.

❖ Optional Features

- Business Class Users
- Journaling – A feature that permanently saves each message that a user sends or receives
- Rights management – Allows a sender to limit recipients' ability to forward or print selected messages.

- In the near future, there will be an optional public folder capability which allows users to share messages in repositories, use team calendars, and to collaborate in a rudimentary way. The public folder functionality will be provided by the Joint Enterprise Portal (JEP) and integrated with JEE.
- At some point, ESD will offer optional migration services, which include migrating users' mailboxes from other mail systems to JEE.

❖ Value to Our Mission Partners

Joint Enterprise E-mail (JEE) is a user-facing IT service intended for the DoD enterprise; it is a scalable and affordable alternative to each of the DoD components deploying and maintaining their own enterprise e-mail service. Adoption of the JEE service will necessarily consolidate e-mail infrastructure, centralize e-mail management, reduce the cost per user, and keep pace with industry functionality and innovation.

❖ Rates/Pricing Information

To find the rates associated with this service, please contact your Enterprise Services Directorate (ESD) Customer Management Executive (CME) team.

❖ Additional Information

DISA has standard performance level data available for our partners to view. Additional data can also be provided as requested. All performance data to be provided will be documented in the SLA which will be executed when the service is ordered.

❖ How to Order

This service can be obtained by working with your ESD CME team to complete a Service Request Form (SRF) that will identify the specifics of your requirement. To obtain contact information for your CME team or the Service Level Management (SLM) hotline, please refer to the Points of Contact.

Additional service and ordering information:

Organization	Contact Information
ESD Phone	CML: 303-224-1660 DSN: 926-1660
ESD Email	CSD_SLM@csd.disa.mil

6.1.2 Joint Enterprise Portal (JEP)

NOTE: This service is still in development.

The Joint Enterprise Portal (JEP) service is a dedicated SharePoint hosting service providing combatant commands (COCOMs), military services, and DoD agencies a flexible, web-based hosting solution which includes a robust set of tools and services to help users manage information and collaborate effectively. Based on the Microsoft SharePoint 2010 platform, this service will provide users with the ability to create and manage mission, community, organization, and user-focused sites for collaboration. Users will be able to manage site collections and content, and distribute allocated storage among their site collections without the additional burden of managing the infrastructure. ESD will manage the multi-tenant environment and provide full lifecycle service for applications, computing, storage, and network infrastructure.

❖ Standard Features

- Global access across the world

- 99.9% availability
- Level II Service Desk support
- CAC enabled authentication
- Content and Records Management (C&RM) in a SharePoint environment
- Online discussion areas, shared document and meeting workspaces, document libraries with version control, and surveys
- Out-of-the-box content management features for documents, records, and web content
- Ability to search SharePoint site content across your block of service or within sub-sites
- Non-Secure Internet Protocol Routing Network (NIPRNet)/Secure Internet Protocol Routing Network (SIPRNet) accessible to private and public content publishing
- Dedicated servers, networks, and physical space in DECCs

❖ Optional Services

- Additional storage to accommodate growth
- Enhanced Enterprise Portal administration tools
- Site-to-site COOP/Disaster Recovery capability

❖ Value to Our Mission Partners

JEP is a dedicated hosting service providing a flexible, web-based hosting solution which includes a robust set of tools and services to help users manage information and collaborate effectively, This service will provide users with the ability to create and manage mission, community, organization, and user-focused sites for collaboration. Users will be able to manage site collections and content, and distribute allocated storage among their site collections without the additional burden of managing the infrastructure. ESD will manage the multi-tenant environment and provide full lifecycle service for applications, computing, storage, and network infrastructure.

❖ Rates/Pricing Information

This service is provided /financed by a Defense Working Capital Fund (DWCF) and will be billed to customers within the rules of stabilized rates. Currently, rates for JEPS are still in development.

❖ Additional Information

DISA has standard performance level data available for our partners to view. Additional data can also be provided as requested. All performance data to be provided will be documented in the SLA which will be executed when the service is ordered.

❖ How to Order

This service can be obtained by working with your Enterprise Services Directorate (ESD) Customer Management Executive (CME) team to complete a Service Request Form (SRF) that will identify the specifics of your requirement.

To obtain contact information for your CME team or the Service Level Management (SLM) hotline, please refer to the Points of Contact.

Additional service and ordering information:

Organization	Contact Information
ESD Phone	CML: 303-224-1660 DSN: 926-1660
ESD Email	CSD_SLM@csd.disa.mil

6.1.3 Defense Connect Online (DCO)

The DCO service is the designated enterprise tool for world-wide synchronous and asynchronous collaboration for both NIPRNet and SIPRNet Networks. DCO is a free/no-cost service provided to all DoD services and agencies that allow users the ability to communicate and share information in a secure forum through the use of instant messaging, low-bandwidth text chat, audio/video web conferencing.

❖ **Standard Features**

Connect 7.0 includes new functionality that enriches online communication and collaboration, enabling organizations to offer more engaging rapid training, and dynamic online meetings. DCO includes the following:

- Integrated VoIP
- Breakout Rooms
- Color Emoticons
- Participant can request "min and video" rights

❖ **Value to Our Mission Partners**

DoD's designated enterprise tool for worldwide synchronous and asynchronous enterprise collaboration. Specific capabilities include web-based conferencing, instant m**ess**aging, whiteboarding, and application sharing. DISA intends on integrating DCO with its video service.

❖ **Additional Information**

You must have a Common Access Card (CAC) in order to register for a DCO account.

How to Register:

- NIRPNet Registration:
  1. Go to the website: https://www.dco.dod.mil.
  2. Accept the agreement.
  3. Enter your CAC pin number in the CAC pin logon field.
  4. Click Logon.
  5. Select Create new account.
  6. Complete all required fields, and then click Submit.

- SIPR Registration:
  1. Must have NIPR DCO to request access to SIPR DCO.
  2. Go to NIPR DCO homepage: https://www.dco.dod.mil.
  3. Logon with your account information.
  4. At top right of the screen, click on **My Account**.
  5. Click on **request SIPR account**.
  6. Fill out required fields, and then click **Submit**.
  7. It will take 24 to 48 until account information is sent to your SIPR email

- Sponsored Accounts:
  1. Sponsored accounts can be created for users who do not have a Common Access Card (CAC) by a valid DCO account holder. Sponsored accounts must have a *.gov (*.sgov.gov) extension.
  2. Go to NIPR DCO homepage: https://www.dco.dod.mil.
  3. Logon with your account information.
  4. At top right of the screen, click on **Sponsored Account**.
  5. Click on desired account; either **request SIPR account** or **request NIPR account**.
  6. Fill out required fields, and then click **Submit**.

Organization	Contact Information
ESD	PEOGES@disa.mil

6.1.4 Strategic Knowledge Integration Web (SKIWeb)

DISA provides access to Strategic Knowledge Integration Web (SKIWeb) (pronounced Sky-Web), which is accessible on SIPRNet and provides a net-centric, asynchronous, collaborative event management capability that includes features and capabilities designed to reduce information overload and improve user effectiveness at the Enterprise level. The SKIWeb user-base is very widespread, ranging from Combatant Commanders such as DRUSSTRATCOM, Joint Staff Chiefs of Staff decision makers, and general action offers. The user base covers over 200 commands, agencies, and organizations to include coalition partners via the Releasable Domain. Any worldwide SIPRNet or JWICS user, that has a vested interest in, or can inject pertinent information on an event of interest, is a potential SKIWeb user. Since introduction by USSTRATCOM, SKIWeb has evolved into one of the DoD's most widely utilized web-based tools and used to rapidly gather and disseminate critical information in real world events such as natural disasters, terrorist attacks, as well as day-to-day activities. SKIWeb is rapidly gaining a reputation as a valuable strategic decision support tool throughout the DoD and among a growing list of strategic allies.

- **Standard Features**

  SKIWeb is a Web application that allows individuals to create events which are real-world and exercise-related occurrences that are of interest to the warfighter community; these events can range from staffing activities to full-blown military engagements. Any user within SKIWeb can generate an event and comment (sometimes referred to as a blog) on events as a situation progresses. This combination of event and related comments builds situational awareness and knowledge. The cooperative efforts of the entire warfighter community can provide situational awareness on a scale never before envisioned and can supply decision makers with even the smallest details necessary to make informed, accurate decisions.

- **Value to Our Mission Partners**

  SKIWeb provides decision and event management support to all levels of a widespread user base ranging from Combatant Commanders to the Joint Staff to Coalition partners on the SIPRNet. The individual suite of capabilities within the portfolio of services provides the user with the flexibility to couple the services in varying ways that support their mission needs. This flexibility provides unprecedented access to web and application content, critical imagery, intelligence and warfighter information, and forward-cached critical data in a secure environment.

- **Optional Features**

  N/A

- **Rates/Pricing Information**

  This service is provided with no charge to the user.

- **Additional Information**

  N/A

❖ **How to Order**

To Gain Access:

https://skiweb.ges.smil.mil
https://m.skiweb.ges.smil.mil
https://skiweb-rel.ges.smil.mil

Organization	Contact Information
ESD	PEOGES@disa.mil

6.1.5 Defense Messaging Service

This service provides a range of assured services to our partner communities that include the military services, DoD agencies, COCOMs, non-DoD U.S. government activities, and the Intelligence Community (IC). These services include the ability to exchange official information between military organizations and to support interoperability with Allied nations, non-DoD activities and the IC operating in both the strategic/fixed-base and the tactical/deployed environments. This service supports up to and including Top Secret Collateral (TS/C) security classification.

❖ **Standard Features**

- Guaranteed Message Delivery – all recipients of a message receive the message or the service returns a non-delivery notification to the message originator giving the reason for each unsuccessful delivery attempt.
- Priority Transmission – Defense Messaging Service (DMS) servers allow users to specify the precedence of each message they originate subject to controls that limit the precedence levels at which each user is authorized to originate a message.
- Message Confidentiality, Integrity, and Non-Repudiation – DMS guarantees this feature through NSA-approved message cryptography and link encryption with audit mechanisms that support non-repudiation.
- Security Access Control – DMS applies these protections to messages based on the message security label and the authorizations assigned to organizations and specific users within those organizations.
- Interoperability – This feature is supported between DoD organizations, non-DoD organization, and allied nations.
- Automated Message Handling -Operated by the user community and implement message dissemination, storage, search, and retrieval.
- High Service Availability – The system provides a high level of service availability based on equipment, communication redundancy path, COOP sites and alternate routing designs.
- High Security Assurance – The system provides a high degree of security assurance based on strict compliance with security policies and directives, as well as, on the use of the NSA-approved and supported cryptographic suite.

❖ **Value to Our Mission Partners**

DMS provides organizational messaging. DMS provides a range of assured services to our partner communities that include the military, services, DoD agencies, COCOMs, non-DoD U.S. government activities, and the Intelligence Community (IC). These services include the ability to exchange official information between military organizations and to support interoperability with allied nations, non-DoD activities and the intelligence community (IC) operating in both the strategic/fixed-base and the tactical/deployed environments. This service supports up to and including Top Secret Collateral

(TS/C) security classification. DMS server enables users to specify the precedence of each message they originate subject to controls that limit the precedence levels at which each user is authorized to originate a message. There are no plans to evolve the current service.

❖ **Rates and Pricing Information**
Service rate information is located under Inventory and Billing on DISA Direct at: https://www.disadirect.disa.mil.

❖ **Other Information**
- Partners order DMS service from Service or Agency operated Area Control Centers (ACCs). The Services/Agency ACCs establish connectivity to the DMS infrastructure in accordance with DMS Interim Procedure 09-V15 (Procedures and Guidelines for Establishing DMS Organizational Users dated 28 March 2008.
- The DGSC serves as POC for Organizational Messaging.

Organization	Contact Information
DGSC	CML: (800) 554-3476 or (614) 692-4790 DSN: (510) 376-3222 or (312) 850-4790
DGSC Email	SBU IP Data Email: DGSC@CSD.DISA.MIL Secret IP Data Email: DGSC@cols.csd.disa.smil.mil

6.1.6 Automated Time, Attendance and Production System(ATAAPS)

The Automated Time, Attendance and Production System (ATAAPS) is a web-based application that provides an online facility for the entry, update, concurrence and certification of time and attendance data for civilian employees of various DoD agencies. It serves primarily as a data entry and repository system, which then feeds payroll data to the DoD payroll system. DISA provides our partners with unique application and Service Desk support. DISA currently supports over 83,779 user accounts.

❖ **Standard Features**
This service provides labor and leave reporting and accountability. It directly interfaces with the Defense Finance and Accounting Service (DFAS) for payroll processing.

❖ **Rates/Pricing Information**
To see the DoD-approved rates for this service, please refer to:
http://www.disa.mil/Services/~/media/Files/DISA/Services/Computing/Rates.pdf

❖ **Additional Information**
DISA has standard performance level data available for our partners to view. Additional data can also be provided as requested. All performance data to be provided will be documented in the SLA which will be executed when the service is ordered.

❖ **How to Order**
This service can be obtained by working with your Enterprise Services Directorate (ESD) Customer Management Executive (CME) team to complete a Service Request Form (SRF) that will identify the specifics of your requirement.

Coming Soon – Online Ordering!

To obtain contact information for your CME team or the Service Level Management (SLM) Hotline, please refer to the Points of Contact.

Organization	Contact Information
ESD Phone	CML: 303-224-1660 DSN: 926-1660
ESD Email	CSD_SLM@csd.disa.mil

6.1.7 FORGE.MIL

Forge.mil is a family of enterprise services provided to support the DoD's technology community. The service provides for collaborative development and IT project management through the full application lifecycle. Forge.mil also enables the reuse of open source and DoD community source software. Forge.mil continues to add new capabilities to support the full system life-cycle and enable continuous collaboration among all stakeholders including developers, testers, certifiers, operators, and users. It is available as an open service supporting anyone affiliated with the DoD, or as a private service and is maintained on both the unclassified and classified networks.

❖ **Benefits**

Forge.mil is designed as an enabler to improve the ability of the DoD to rapidly deliver dependable software, services, and systems in support of net-centric operations and warfare by:

- Enabling cross-program sharing of software, system components, and services
- Promoting early and continuous collaboration among all stakeholders (i.e., developers, material providers, testers, operators, and users) throughout the development life-cycle
- Connecting users, team members, program and community leaders, and subject matter experts making a difference in Information Technology Acquisition
- Providing a forum for users to share knowledge, experience, and lessons learned on how to improve and accelerate software development and deployment
- Rapidly delivering effective and efficient development and test capabilities for DoD technology development efforts
- Helping to protect the operational environments from harmful systems and services
- Encouraging modularity so that large programs to be developed, fielded, and operated as a set of independent components can evolve and mature at their own rates
- Eliminating duplicative testing and improving dependability by adopting common test and evaluation criteria supported by standard testing tools and methods
- Greatly reducing the time and cost required to develop useful, dependable systems for the warfighters

❖ **Current Offerings**

- **Forge.mil Community** is a collaborative content and knowledge management site for Forge.mil users to connect and share information using social collaboration tools such as group blogs, discussions, wiki, documents and polls.
- **SoftwareForge** enables the collaborative development and distribution of open source software and DoD community source software.
- **ProjectForge** provides the same application life cycle management tools to DoD projects and programs as SoftwareForge, but for programs and/or projects that are not doing DoD community source development and/or need to restrict access to specific project members.

▪ **Value to Our Mission Partners**

Forge.mil supports agile software development (or can be tailored to support other development methodologies) and software reuse on NIPRNet and SIPRNet. Forge.mil provides a 'DoD-internal' collaborative development environment with application lifecycle management tools such as software version control, bug/issue tracking, requirements management, and project reporting as well as

collaboration tools such as project wikis, discussion forums, project mailing lists and document management. These capabilities allow geographically dispersed project team members to securely access and manage all project assets in a single location. The system currently enables the collaborative development and use of open source and DoD community source software. These initial software development capabilities are growing to support the full system life-cycle and enable continuous collaboration among all stakeholders including developers, testers, certifiers, operators, and users. It is available as a community service, or as a private service on both the unclassified and classified networks.

❖ **Additional Information**
Additional information on the features and capabilities of Forge.mil can be found at: www.forge.mil, or by contacting the FORGE.mil Community Management Team at: "community@forge.mi"l.

❖ **Rates/Pricing Information**
Forge.mil Community and SoftwareForge are offered with no charge to anyone affiliated with the DoD as a value added enterprise service.

To register you will require a DoD Common Access Card (CAC) or an External Certification Authority certificate (ECA cert) with DoD sponsorship.

6.2 Infrastructure

6.2.1 Rapid Access Computing Environment (RACE)

RACE provides a streamlined process for the provisioning and subsequent development, testing, and through the utilization of Enterprise Mission Assurance Support Service (eMASS) and VMS, streamlined certification, accreditation and deployment of applications to a DISA DECC. DISA packages hosting, networking, security and connectivity together as a service. RACE is available to all our DoD partners as well as their corporate design partners. Users can acquire server capacity rapidly, for short or long-term use, using Operations and Maintenance (O&M) or Research, Development, Test & Evaluation (RDT&E) funding, without the need for capital acquisitions.

❖ **Standard Features**
The following features are included in the rates. Authorized partners may:
- Procure and provision virtual servers using a self-service web portal
- Use the development and test and development (T&D) servers within 24 hours of receipt of payment
- Use the follow-on comparable production servers available within seven (7) to 10 days of receipt of payment and completion of Certification and Accreditation (C&A) paperwork.

❖ **Value to Our Mission Partners**
RACE services offer virtualized computing resources as a service, i.e., a DISA version of IaaS. RACE provides a user self-service ordering capability for development and test environments that can be purchased on-line and provisioned rapidly. RACE allows authorized users to order virtual servers and storage using drop-down menu selections on a web portal. Automated and semi-automated backend systems validate user information, build the server images purchased, and send emails to the RACE user with the IP addresses, usernames, and associated passwords that enable users to access the servers and install their own software and applications. The Rapid Access Computing Environment (RACE), a cloud service, provides a streamlined process for the provisioning and subsequent development; testing; and through the utilization of Enterprise Mission Assurance

Support Service (eMASS) and VMS, streamlined certification, accreditation and deployment of applications to a DISA DECC.

❖ **Rates/Pricing Information**
To see the DoD-approved rates for this service, please refer to:
https://cd22projects.csd.disa.mil/warning.jsp

❖ **Additional Information**
For additional information please visit: http://disa.mil/race/

❖ **How to Order**

This service can be ordered and paid for directly on the RACE portal at http://disa.mil/race/.

To obtain contact information for your Customer Management Executive (CME) team or the Service Level Management (SLM) hotline, please refer to the Points of Contact.

6.2.2 Global Content Delivery Service (GCDS)

GCDS provides a DISN enterprise- level service to accelerate delivery and improve reliability of web applications. GCDS is a globally distributed computing platform comprised of a mesh network of content delivery nodes deployed across the DISN, including both Non-Classified Internet Protocol Routing Network (NIPRNet) and Secret Internet Protocol Routing Network (SIPRNet). GCDS leverages commercial Internet best practices to provide state-of-the-art web content and web application delivery via standard web protocols, hypertext transfer protocol (HTTP) and hypertext transfer protocol secure (HTTPS).

The technology behind GCDS leverages proprietary routing algorithms that dynamically and optimally route traffic across the DISN, even as network conditions change. GCDS provides services to end users at the edge of the DISN including network optimization featuring:

- Transmission Control Protocol (TCP) optimization – One of the core protocols of the Internet Protocol Suite
- Object pre-fetching – A method that can expedite the presentation of web pages by utilizing the current web page's view time to acquire the web objects of future web pages
- Persistent connections – Links that do not close when the execution of a web page script ends
- Secure Socket Layer (SSL) off-load – Procedure transfers a portion of SSL processing duties, normally handled by servers, to a separate, specially designed device
- Content delivery services
- Reporting and monitoring services such as traffic reports and alerts.

GCDS is fully accredited with Authority to Operate (ATO) and continues to expand its reach and capabilities to soon include network repository, global load balancing, video/audio streaming, and Java 2 Enterprise Edition (J2EE) support.

An additional service of the GCDS program management office (PMO) is the System Network Availability Performance Service (SyNAPS). All our partners purchasing GCDS are provided performance metrics from SyNAPS and can access their sites' performance data/reports via a partner portal. Two SyNAPS transactions per digital domain uniform resource locator (URL) are available to our GCDS partners at no additional charge. An example of the two free transactions can include a performance/availability metric on a screen or keystroke pattern. The report can show the transaction's metrics for the partner's origin

site and GCDS (two transactions). If the partner wants additional transactions, they can be purchased separately.

❖ **Standard Features**

DISA will plan the deployment logistics, expected service levels, and other program specific criteria. The managed service provider will provide the servers to DISA for GCDS as well as all related software and assist with network design and installation of the servers.

The roles and responsibilities of the managed service provider include the following:

- Monitoring and managing of the infrastructure networks and equipment
- Professional services, integration services, and partner care (including Service Desk)
- Local system administration (SA) and remote group administration of the GCDS global network.
- Two SyNAPS transactions per digital domain URL

GCDS will deliver content that is developed and maintained by the application/content owner. The transmission must process through port 80 (HTTP) or port 443 (HTTPS). GCDS is not a hosting environment but an expansion of the web applications infrastructure. GCDS minimizes or eliminates the requirement to forward deploy additional servers and personnel to reach the targeted audience. The application/content owners will assume all responsibilities associated with the development, initial installation, testing, and contingency operations decisions for the content, and are ultimately responsible for the security of the platforms they manage.

❖ **Optional Features**

GCDS NetStorage – One of the main goals of DoD organizations providing mission critical content on the NIPRNet or SIPRNet is to offer the best end-user experience possible to aid the warfighter. This can be achieved by quickly and reliably delivering rich media files. However, storing and maintaining a large collection of on-demand files, including electronic images, geo-spatial imagery, streaming media files, software, documents, and other digital objects is both technically challenging and resource intensive. It requires a significant investment in racks of redundant servers as well as constant upkeep, including the management of administrative details.

GCDS NetStorage is not local storage normally housed in a DECC, but is storage within the Cloud available to all GCDS nodes worldwide.

GCDS NetStorage is a secure, DoD enterprise solution that eases the burdens associated with data storage. NetStorage consists of multiple terabytes of storage capacity, geographical distribution/replication, a massively scalable architecture, and proprietary mapping and routing technology. By using this fault-tolerant storage service, our partners can make their rich media content available to users on demand, anytime and anywhere.

❖ **Value to Our Mission Partners**

GCDS provides a DISN enterprise-level service to accelerate delivery and improve reliability of web applications.

❖ **Rates/Pricing Information**

Service rate information is located under Inventory and Billing on DISA Direct at: https://www.disadirect.disa.mil

❖ **Additional Information**

For additional information on GCDS please go to: http://www.disa.mil/Services/Computing/GCDS

❖ **How to Order**

Additional service and ordering information:

Organization	Contact Information
ESD Phone	CML: 303-224-1660 DSN: 926-1660
ESD Email	CSD_SLM@csd.disa.mil

6.2.3 Enterprise Service Monitoring

Enterprise Service Monitoring (ESM) is a core capability to monitor and manage the performance and operational status of Web Services. It is integrated with existing network, system, and security management capabilities to provide effective situation awareness.
ESM collects and stores performance data about web services using agents (centralized, or deployed in a partner's environment). Using this data you can fine-tune the service or determine where resources should be used to improve overall service performance. Historical data helps establish baseline performance measurements for ongoing monitoring and alerting. Monitoring multiple web service instances may indicate the need to implement or tune load-balancing, failover, and throttling policies.

- **Standard Features**
  DISA ESM provides many features that can be leveraged by the Service Provider. The ESM features include:
  - Track operational status and performance overtime
  - Real-time access to service metrics, Service Level Agreements (SLA), and service status
  - Customer email alerts about customer's service
  - Report generation covering quarterly, monthly, weekly, and/or daily availability and performance. You pick the timeframe and all the other parameters.
  - Minimize negative customer impact
  - Speed time-to-fix
  - Integrating with GIG NetOps

- **Optional Features**
  NA

- **Rates/Pricing Information**
  No charge

- **Additional Information**
  NA

- **How to Order**
  Additional service and ordering information:

Organization	Contact Information
ESD	PEOGES@disa.mil

6.2.4 Data Services Environment

The Data Services Environment (DSE) is an enhanced dashboard that brings together Service Oriented Architecture (SOA) capabilities into a common, modular framework. Its goal is to simplify the publication and discovery of data services that facilitate information sharing across the Department of Defense. The

following products are part of the DSE - the Metadata Registry (MDR), Service Discovery (SD), Net-Centric Publisher (NCP) and the Enterprise Authoritative Data Source (EADS).

❖ Standard Features

All Web Hosting Levels include the following services:

- The Metadata Registry (MDR) is used for the collection, storage and dissemination of structural metadata information resources (schemas, data elements, attributes, document type definitions, style-sheets, data structures etc.). This Web-based repository is designed to also act as a Clearinghouse through which industry and government coordination on metadata technology and related metadata issues can be advanced. As OASD's Executive Agent, DISA maintains and operates the DoD Metadata Registry under the direction and oversight of DOD CIO.
- Service Discovery (SD) allows users to search the Enterprise Service Registry for Service Providers and Services. Users within the DoD Enterprise can discover and leverage various enterprise service offerings. Developers can locate information such as service offers, service specifications, and taxonomical information, and they can readily reuse these existing entities to save time and avoid duplication of effort.
- Net-Centric Publisher (NCP) is a tool that provides users with a simplified workflow for publishing metadata to the DSE Metadata Environment. In the Department's transition to net-centricity, it has become increasingly apparent that the underlying metadata infrastructure required to support net-centric operations is complex, involved, and not clear to many of our users. The interdependencies of metadata in the Department's service-oriented path to net-centricity is not well understood by those who need to make their asset metadata visible, accessible, and understandable in order to comply with DoD Net-Centric Data Strategy objectives. The Net-Centric Publisher pushes that complexity further from the user by providing a clear set of workflows and a single interface point for publishing metadata to the DSE Metadata Environment.
- Enterprise Authoritative Data Source (EADS) provides one-stop access to DoD data source directories to improve search, access, consistency, and integration of data services as well as to increase collaboration amongst data producers and consumers.

❖ Value to Our Mission Partners

The Metadata Registry is a central, federation-capable site for the publication and distributed management of metadata. It is a virtual "place" where collections of metadata components, in which DoD organizations and others have invested, can be: published, made visible, accessible, and understandable to large audiences; transparently and collaboratively evolved and otherwise managed by representatives of a large, diverse, geographically distributed group of people and organizations; monitored to determine contextual relevance (importance/priority), quality, usage and other factors that affect engineering and resourcing (future investment) decisions; and exploited by the machine-to-machine process in support of such functions as validation and transformation.

Service Discovery is DoD's designated enterprise tool for worldwide content discovery. It allows the user to define their search criteria and discover content provided via a centralized search engine, federated data sources, and the Enterprise Catalog.

Enterprise Authoritative Data Source acts as a key enabler to make data "visible, accessible, and understandable". It provides: greater data visibility and accessibility by implementing an Enterprise service; reduces cost and improves timeliness through the consolidation of EADS; eliminates the need to stand up and manage individual registries' streamlines search and access; and provides a set of tools to register and discover data services across the Department.

❖ **Additional Information/How to Order**
Additional service and ordering information:

Organization	Contact Information
ESD	PEOGES@disa.mil

6.3 Identity Management

6.3.1 DoD Visitor

DoD Visitor is a joint effort of the Department of Defense Chief Information Officer (DoD CIO), the Joint Staff, the Defense Information Systems Agency (DISA), the National Security Agency (NSA), and the Defense Manpower Data Center (DMDC). The vision of Enterprise User is to deliver the following capability to every DoD user:

"I can go anywhere in the DoD, login, and be productive."

DoD Visitor will be deployed on NIPRNet/SIPRNet Windows Domain Controllers supporting end-user device login.

❖ **Standard Features**
The following minimum functionality and services will be available to a DoD Visitor:
- Access to the network through Microsoft Internet Explorer
- Access to basic Microsoft Office applications (Word, PowerPoint, and Excel), and to Adobe Acrobat Reader
- Access to currently installed local printers (from within the above applications)
- Temporary storage on the desktop and My Documents folder

❖ **Optional Features**
N/A

❖ **Value to Our Mission Partners**
A functionality that enables any DOD NIPRNet domain with Microsoft Windows Domain Controllers supporting user accounts and authentication to provision an account to any visiting (i.e. has no account) user that presents a valid CAC/PKI certificate. The account has limited privilege and is intended to primarily provide the user with browser access to the NIPRNet.

❖ **Additional Information**
You must have a Common Access Card (CAC) in order to register for a DCO account.

❖ **Rates, Pricing, and Additional Information**

Organization	Contact Information
ESD	PEOGES@disa.mil

6.3.2 Enterprise Access Control (PEP/PDP)

The Enterprise Access Control is a combination of open source Policy Decision Point (PDP) and Policy Enforcement Point (PEP) to assist users in developing an ABAC solution applicable to all US DoD

systems (Unclassified and Classified). These components are part of the Access Control Infrastructure and are provided as an interim solution. Activities are underway to offer a complete solution.

❖ **Standard Features**
- The PDP applies relevant access control policies to a request and returns an access control decision.
- The PEP intercepts a resource access request; creates a corresponding request for the PDP and enforces the PDP's access control decision by either passing the original request to the resource or by sending an appropriate error code back to the requesting service.

❖ **Rates/Pricing Information**
This service offering is a reference implementation; there is no fee to download.

❖ **Additional Information**
N/A

❖ **How to Order**
Additional service and ordering information:

Organization	Contact Information
ESD	PEOGES@disa.mil

6.3.3 Enterprise Identity Attribute Services

The DoD Enterprise Identity Attribute Service (EIAS) serves to distribute DoD person, persona and personnel attributes to applications and services in a controlled, consistent, and secure manner. The information provided via EIAS can be used to confirm an individual's identity and affiliation to the DoD for the purpose of enabling Attribute Based Access Control (ABAC). The EIAS is managed by the Defense Manpower Data Center (DMDC).

❖ **Standard Features**
- The EIAS provides current DoD affiliation data to customers who have a business justification and a need-to-know to receive person and personnel-based attributes for authentication and authorization. EIAS leverages real-time Web service technologies to distribute a common set of data attributes utilizing signed SAML 2.0 in all EIAS requests and responses.

❖ **Rates/Pricing Information**
- There is currently no fee to use the service; however, creating an interface to EIAS requires client-side development that requires coordinated with the DMDC Identity Web Services implementation team.

❖ **Additional Information**
- The EIAS User Integration Guide assists the user community with the complete process of developing an interface to the service. The guide describes the business and technical requirements required by DMDC to become fully operational with EIAS. The EIAS integration guide can be found at the following intelink site: https://www.intelink.gov/wiki/Enterprise_Identity_Attribute_Service.

❖ **How to Order**

- Additional service and ordering information:

Organization	Contact Information
ESD	PEOGES@disa.mil

7 Information Assurance

7.1 Policy and Guidance (IA Standards and Training)

IA standards and training developed for and used throughout DoD to secure computing devices and increase cyber defense awareness.

❖ **Standard Features**

- IA Standards and Training features FSO provides in support of secure computing for the war-fighter's networks and systems.
- STIG/Checklist Development – Develop STIG or Checklist to support a specific technology or situation. This will be sufficient to provide configuration settings and parameters for the assured operation within the DOD environment.
- STIG/Checklist Maintenance – Maintain STIG and Checklist to respond to technology changes.
- Develop Training – Develop IA training for a specific system or function.
- Maintain Training – Maintain IA training for a specific system or function based on technology and procedural changes.
- Training Management Support – Conduct training needs assessments, schedule classes, provide logistics for the conduct of the classes, and collect and evaluate feedback.
- Conduct Training – Conduct on-site IA classroom training.
- IA Support Environment (IASE) Support – Manage the IASE. This includes content management and at times collaboration facilitation.
- IA/IT Policy Review – Review IA and IT policy and directives for feasibility and applicability to the DISA IA mission support area.

❖ **Rates/Pricing Information**

- In Fiscal Year 2013, FSO is proposed to become a DWCF entity. As such, the cost of many services will be billed directly to service recipients based on an OSD Comptroller rate schedule.
- Currently, the cost is assigned to appropriated funds or billable directly to service recipients on a cost reimbursable basis. To determine which applies, contact the POC below.

❖ **Additional service and ordering information can be found by emailing or calling FSO.**

Organization	Contact Information
FSO Phone	CML: 717-267-9876 DSN: 570-9876
FSO Email	FSO_SLM@disa.mil

7.2 Compliance Inspections

Compliance Inspections consist of conducting formal certification reviews and supporting other aspects of the risk management process, conducting cyber readiness inspections on behalf of United States Cyber Command (USCYBERCOM), and coordinating Net Assurance activities across DISA and COCOMs.

❖ Standard Features

The features of this service included distinct inspections, reviews and assessments which FSO can provide to assure your IA integrity and compliance with DoD IA Certification and Accreditation Process (DIACAP) and other regulations.

- Command Cyber Readiness Inspection (CCRI) – A formal inspection conducted under the direction of USCYBERCOM's Enhanced Inspection Program.
- Security Assistance Visits (SAVs) – A process by which DISA FSO personnel will conduct an on-site assessment and validation of compliance with mandated IA, CND, certification and accreditation (C&A), or other focus areas either as a standalone effort or in preparation for a scheduled inspection or evaluation.
- CNDSP Level II Inspections – CNDSP evaluations are an on-site evaluation and validation of compliance with mandated CND Service requirements as outlined in DoD O-8530.1 and DoDI O-8530.2.
- CNDSP Level II Designation Assessments – CNDSP validations are a review and validation of alignment to an accredited CNDSP. A formal recommendation is provided upon completion of the on-site evaluation.
- IA Readiness Reviews (IARRs) – A formal review in 12 IA areas to determine a site's current IA program status and provide formal recommendations for improvements in areas where deficiencies or non-compliance are discovered.
- Enclave and System Certification – Can provide on-site technical assessments and certifications recommendations to a Designated Approving Authority (DAA) in support of enclave accreditation, coalition enclave or systems.
- Combatant Command (COCOM) exercise support – DISA provides critical exercise support for the COCOMs in various theater and global exercises. This support can come from a variety of areas and include CND technology Subject Matter Experts (SMEs), CND Integrators, and CND analysts.

❖ Rates/Pricing Information

- In Fiscal Year 2013, this service will become a DWCF entity. As such, the cost of many services will be billed directly to service recipients based on an OSD Comptroller rate schedule.
- Currently, the cost is assigned to appropriated funds or billable directly to service recipients on a cost reimbursable basis. To determine which applies, contact the POC below.

❖ How to Order

Other service and ordering information can be found by emailing or calling FSO.

Organization	Contact Information
FSO Phone	CML: 717-267-9876 DSN: 570-9876
FSO Email	FSO_SLM@disa.mil

7.3 Capability Implementation

Capability Implementation consists of operationalizing IA products to ensure a smooth transition from the development process to an operational environment.

❖ **Standard Features**

Capability implementation features in support of IA material solutions about to be fielded.

- Implementation – The fielding and implementation of Computer Network Defense (CND) technologies into the operational environment to support Tier 2 and 3 CND Service Provider (CNDSP).
- Configuration Management – The configuration management (CM) processes associated with new and existing CND technologies utilized to support operations for Tier 2 and 3 CNDSP. Activities involve baseline maintenance, system administration, and vulnerability management.
- Product Concept of Operations (CONOPs)/Tactics, Techniques, and Procedures (TTPs) Development – The development of capability solutions with CONOPs solutions and supporting TTPs. These documents are developed for all roles including: users, operators, analysts, system administrators, etc.
- Deployment, Implementation, Maturization & Effectiveness (DIME) – Standard methodology and vendor services for gaining resource efficiencies and achieving full solution operationalization across DoD.
- Vulnerability Management System (VMS) Operations – VMS operations support current VMS partners and provide operationalization support to new and current VMS partners.

❖ **Rates and Pricing Information**

In Fiscal Year 2013 this service will become a Defense Working Capital Fund (DWCF) entity. As such, the cost of many services will be billed directly to service recipients based on an Office of the Secretary of Defense (OSD) Comptroller rate schedule.

Currently, the cost is assigned to appropriated funds or billable directly to service recipients on a cost reimbursable basis. To determine which applies, contact the POC below.

❖ **Additional service and ordering information can be found by emailing or calling FSO**

Organization	Contact Information
FSO Phone	CML: 717-267-9876 DSN: 570-9876
FSO Email	FSO_SLM@disa.mil

7.4 Network Defense

DISA provides Network Defense capabilities including features needed to ensure warfighter success through secure networks.

❖ **Standard Features**

- Network Security Monitoring & Incident Reporting & Attack, Sensing, and Warning (AS&W) – Service provided to CNDSP subscribers which utilizes an incident reporting system for complete

and meaningful incident report recording and rapid distribution to DoD channels and law enforcement/intelligence communities.

- Incident Response and Recovery Team (IRRT) – Deployable emergency response team designed to assist sites in locating and recovering from network intrusions.
- System Architecture, Analysis and Testing (SAAT) – Test the security and stability of the associated program using a variety of techniques.
- Malware Analysis – Reverse engineering of malware to determine the functionality of the software and to identify artifacts that can be utilized to locate additional infections.
- Media Analysis – Analysis performed on system media to identify attack vectors, tools used, exploited software, and increase detection ability on networks and hosts.
- Trends Analysis – Detailed analysis of IA/CND data from varying sources, to include compliance and intrusion data to identify and analyze trends, creating value-added products and reports for the enhancement of IA/CND policies, technologies, tactics, and training products.
- CNDSP Exercise Support – Provides critical IA-based exercise support in various theater and global exercises.
- Red Teaming – The Red Team is a focused, threat-based operation by an interdisciplinary, simulated adversary to expose and exploit vulnerabilities as a means to develop recommendations for the improvement of the security posture and operational CND capabilities and procedures utilized to protect networks and systems.
- Penetration Testing – Involves approaches to vulnerability identification, enumeration, and attempted exploitation to determine the value and effectiveness of a network, system, or application's security configuration. Penetration testing is coordinated and conducted primarily in the open in accordance with a signed authorization by the system owner.
- Vulnerability Assessment, Analysis & Trending – Vulnerability Assessment, Analysis, and Trending is conducted at the request of network owners in support of, or in augmentation to, the partner's internal, DoD mandated vulnerability scanning and assessment actions.
- Non-materials Solutions Development – The rapid development of tactical capabilities in response to an emerging threat.
- IA Training Program Support – Provides hands-on technical assessment training for networks, operating systems and applications.
- CNDSP Subscriber Services Support – Options for all or partial CNDSP Tier 2 services (Protect, Detect, Respond and Sustain)
- Sensor Implementation – The fielding and implementation of CND technologies into the operational environment in support of Tier 2 and 3 CNDSP.
- Sensor Configuration Management – Configuration and baseline support for managed sensors.
- Sensor CONOPs/TTP Development – Development of CONOPs for sensor solutions and supporting TTPs.
- Sensor Trouble Desk Escalation – Trouble shooting assistance for sensor issues that surface from the sensor grid.

❖ Rates and Pricing Information

In Fiscal Year 2013, FSO is proposed to become a DWCF entity. As such, the cost of many services will be billed directly to service recipients based on an OSD Comptroller rate schedule. Currently, the cost is assigned to appropriated funds or billable directly to service recipients on a cost reimbursable basis. To determine which applies, contact the POC below.

❖ **Additional service and ordering information can be found by emailing or calling FSO**

Organization	Contact Information
FSO Phone	CML: 717-267-9876 DSN: 570-9876
FSO Email	FSO_SLM@disa.mil

7.5 Secure Configuration Management

The Secure Configuration Management (SCM) program manages security features and assurances through control of changes made to the hardware, software, firmware, documentation, test, test fixtures, and test documentation throughout the life cycle of an information system.

SCM relies upon performance, functional, and physical attributes of IT platforms and products and their environments to determine the appropriate security features and assurances that are used to measure a system configuration state.

SCM was established as part of the larger Enterprise Security Management (ESM) initiative. The roles and responsibilities for the SCM Program Management Office (PMO) were defined, such that, the National Security Agency (NSA) has primary responsibility for advanced technology R&D efforts and DISA has systems engineering and Operations and Maintenance (O&M). Since the establishment of the SCM program, many operational requirements have been directed and defined to automate enterprise vulnerability and configuration management assessment and reporting activities.

7.5.1 Assured Compliance Assessment Solution (ACAS)

The Assured Compliance Assessment Solution (ACAS) is an integrated software solution that is scalable to an unlimited number of locations. The solution's tiering ability will give Department of Defense (DoD) enhanced enterprise security while being easy to install and manage. It can be easily deployed via download to all DoD agencies – without the need to procure and install appliance devices. DoD will discover that the ACAS product suite easily provides the required automated network vulnerability scanning, configuration assessment, application vulnerability scanning, device configuration assessment, and network discovery it needs. Further, the product suite generates the required reports and data, with a centralized console, and is SCAP compliant. There is much more to the capabilities of the ACAS and you can find out more information by reading the material referenced below.

❖ **Standard Features**

- **Security Center**

As the central console for ACAS, Security Center offers the ability to automate and quickly scale an organization's vulnerability and compliance scanning infrastructure, as well as provide capabilities to allow for management, alerting, and reporting against vulnerability and compliance requirements.

- **Nessus User Interface**

A fully capable scanner covers a breadth of checks, including unique Common Vulnerabilities and Exposures (CVEs), and successfully operates across different environments.

- **xTool**

The X-Tool converts distributed eXtensible Checklist Configurations Description Format (XCCDF) files into Extensible Markup Language (XML) schema, which allows the files to be imported into SecurityCenter and easily customized, if necessary.

- **3D Tool**

The Topology Viewer imports asset data from the Nessus scanner or SecurityCenter and provides graphical analysis information such as network and protocol maps, communication paths, and vulnerability maps. The Topology Viewer also imports and converts Open Vulnerability Assessment Language (OVAL) vulnerability files for upload into SecurityCenter.

- **Passive Vulnerability Scanner**

The PVS monitors network traffic in real-time. It determines server and client side vulnerabilities and sends these to SecurityCenter in real-time. It continuously looks for new hosts, new applications and new vulnerabilities without requiring the need for active scanning.

❖ **Additional Information**

For additional information go to:
https://www.intelink.gov/wiki/Assured_Compliance_Assessment_Solution

7.5.2 Enterprise Network Mapping and Leak Detection Solution

This is an enterprise Commercial Off The Shelf (COTS) solution for network intelligence that provides comprehensive network mapping and leak detection capability with interactive visualization tools for analyzing information on the state of the DoD IT infrastructure. The ENMLDS solution grants discovery across an unlimited count of assets connected to the .mil domain (including both the classified and unclassified networks).

The operational vision of Enterprise Network Mapping and Leak Detection Solution (ENMLDS) is to provide an enterprise leak detection capability as its primary focus, with support for continuous mapping of the SIPRNet and NIPRNet. ENMLDS provides the Services with an automated tool to improve situational awareness and Computer Network Defense (CND) while helping with compliance to the DoD Information Operations Condition (INFOCON) level.

❖ **Standard Features**

- **ENMLDS**

ENMLDS is comprised of four components which provides for scalability and future growth of CND capabilities to fulfill current and future security and management gaps. ENMLDS will empower the network operators and defenders with a graphical mapping of the network interconnections including detailed reporting on each asset discovered across the enclave. The detailed reporting provides information on the quantity, model, operating system version, and interconnection of network assets.

- **Report Server**

Functioning as the data repository, Report Servers separate report generation from scanning to further reduce IPsonar's operational footprint. A single remote Report Server can support multiple Scan Servers.

- **Scan Server**

These resources are positioned at appropriate points in the network to assure that business applications and even the lowest-speed network links are unaffected by IPsonar network traffic. Multiple scans can be run simultaneously.

- **Sensors**

Accurate, complete network scanning is achieved through the use of network entry points called Sensors. These portable entry points provide the flexibility to address even the fastest changing networks.

Online Sensors
Offline Sensors

- **Discovery Types**
  - **Network Discovery**
    Network Discovery proactively identifies the network and its perimeter including address space, hosts, devices and the true interconnectivity of sub-networks throughout the enterprise.
  - **Host Discovery**
    Host Discovery enumerates the IP devices on the active network segments.
  - **Leak Discovery**
    Leak Discovery identifies end-point and network devices that have inbound and/or outbound connectivity beyond the network perimeter to the Internet or other networks via Internet Control Message Protocol (ICMP) and UDP protocols.
  - **Service Discovery**
    Service Discovery leverages information derived from IP stacks to identify current and emerging Internet services and proprietary IP applications active on hosts and devices on the enterprise network.
  - **Device Discovery**
    Device Discovery identifies wireless access points by "banner-grabbing" or probing known management interfaces, specifically Hypertext Transfer Protocol (HTTP) and SNMP based interfaces.

7.5.3 Continuous Monitoring and Risk Scoring (CMRS)

Continuous Monitoring and Risk Scoring (CMRS) allows visibility of cyber risks and demonstrates the ability to use DOD Enterprise security tools and content. The CMRS pilot will assess continuous monitoring capabilities to support a phased pilot implementation. This pilot will leverage implementation efforts from four use cases: IAVM Reporting, CCRI Automation, Certification and Accreditation, and Net Assurance/Ops. This pilot will be used to demonstrate the effectiveness of a risk management approach to cyber security, and the ability to maintain an accurate picture of an organization's security risk posture, provide increased visibility into assets, and leverage automated data feeds to quantify risk.

❖ **Standard Features**

CMRS currently provides several capabilities and services:

- Provides CC/S/A/FAs with a consolidated asset visibility for HBSS managed and unmanaged hosts.
- Scores risks related to Windows STIG and Patch compliance
- Scores risks for Antivirus and HBSS point product compliance
- Provides risk scores for COCOMS, CC/S/A/FA, and/or enterprises

CMRS also leverages the Portable Risk Score Manager (PRSM) tool to view the risk scores for the organization. PRSM utilizes the Operational Attribute Module (OAM) and the Assessment Results Consumer and Analysis Tool (ARCAT) to arrive at the data results displayed in the risk scoring tool.

- Pilot Activities
  CMRS pilot will leverage implementation efforts from four use cases: IAVM Reporting, CCRI Automation, Certification and Accreditation, and Net Assurance/Ops.
- IAVM Reporting Use Case

The IAVM Use Case will be a phased evolution of IAVM reporting to using continuous monitoring capabilities.

Phase 1: preparatory phase in which DISA obtains approval from USCYBERCOM to eliminate singular, manually-entered POA&Ms.
Phase 2: transition phase in which DISA begins using continuous monitoring automated capabilities to report IAVM compliance to USCYBERCOM.
Phase 3: institutionalize phase in which DISA will evolve IAVM reporting to the USCYBERCOM IAVM-Next Generation process (which is based on vulnerability exposures, threats, and impacts).

- CCRI Automation
  CCRIs will leverage continuous monitoring automation in a three phased approach:
  Phase 1: DISA will test existing SCCVI (Network Scanner) automation with VMS to minimize manual data entry efforts during CCRI after action process.
  Phase 2: DISA will deploy Phase 1 capability to DoD as an optional CCRI after action process for all CCRIs.
  Phase 3: CCRIs will perform research and develop way forward to use HBSS and the future network scanner.
- Certification and Accreditation
  The Certification and Accreditation (C&A) continuous monitoring use case is treated as two distinct efforts with a phased approach:
  Effort 1: a four phased approach for DISA to fully integrate HBSS continuous monitoring capabilities into existing C&A process and tools (DIACAP using VMS and eMASS).
  Effort 2: an effort to support the DoD and Federal Government initiatives to transform from current C&A process to a continuous authorization process, modeled after the NIST Risk Management Framework (RMF). The RMF defines a continuous process to assess, authorize, and monitor system risks.
- Net Assurance/Ops
  The Net Assurance/Ops use case will support the development of Operational Capabilities using Continuous Monitoring
  Phase 1: will use existing HBSS continuous monitoring capabilities to assist in the development of trending and data mining requirements.
  Phase 2: will use enhanced data mining capabilities to support the development of OPs countermeasures.
  Phase 3: will train Net Assurance continuous monitoring users to use the data in support of countermeasure efforts.

❖ **Additional Information**

- For additional information please call: 301-225-5301 or refer to:
  https://www.intelink.gov/wiki/Continuous_Monitoring_and_Risk_Scoring

7.5.4 Enterprise Mission Assurance Support Services (eMASS)

Enterprise Mission Assurance Support Service (eMASS) is the Department of Defense's (DoD) recommended tool for information system Certification and Accreditation (C&A). eMASS automates the C&A process, manages workflow among user roles, and generates a variety of reports based on user needs--including all reports required by the DoD Information Assurance Certification and Accreditation Process (DIACAP) and the Federal Information Security Management Act (FISMA).

As directed by DoD Instruction 8510.01, "DoD Information Assurance Certification and Accreditation Process (DIACAP)," dated Nov. 28, 2007, the Director, DISA, under the authority, direction, and control of

the Assistant Secretary of Defense for Networks & Information Integration/DoD Chief Information Officer, shall "provide automated validation capabilities to the DoD components for use in the DIACAP." eMASS is the centerpiece of an ongoing DoD effort to automate a broad range of services for comprehensive, fully-integrated information assurance (IA) management at the DoD Component level, is fully compliant with the concept of IA controls-based information assurance, and is intended to provide full support of the DoD 8500 series.

❖ Standard Features

eMASS is a government-owned, commercial off-the-shelf based solution that seamlessly integrates several capability models to support IA program management (PM) needs. eMASS facilitates robust, measurable IA PM through the following capabilities:

- Security-process management and reporting based on compliance with IA Controls
- Standardized information exchange to facilitate dynamic connection decisions
- Workflow automation
- Simplified management of the entire C&A process from C&A package submission through completion
- Traceable systems-security engineering across the entire system-development life cycle
- Facilitation of regulatory and IA management-reporting requirements, such as those contained in FISMA
- Providing senior leadership visibility into the IA posture of all DoD organizations through the Enterprise Reporting Service (ERS) module.

The overarching vision is to allow all parties with the need to share access to pertinent data in a near-real-time, secure environment. Hence, the ERS module will also serve as the supervisor to determine which reports for each organization get approved by the assigned approver role before they are released to DoD community. These reports are measured by the compliance and severity associated with the implementation of IA controls applied to their respective accreditation packages.

❖ Additional Information

okcpeoservicedesk@csd.disa.mil
(405) 739-5600, Option 3
(DSN 339-5600, Option 3

And:
http://www.disa.mil/Services/Information-Assurance/EMASS/Get-EMASS

❖ How to Order

eMASS Capacity Approval Process

Organizations interested in deploying an eMASS implementation must first coordinate this deployment with the appropriate Military Department, Combatant Commanders, Defense Agency, or Defense Field Agency Chief Information Officer (CIO) (e.g., Department of the Navy CIO, Marine Corps CIO, Army CIO/G6, Office of Warfighting Integration and Chief Information Officer, Joint Chiefs of Staff J6, Office of the Secretary of Defense CIO, etc.) – reference Department of Defense Directive (DoDD) 8000.1 (Management of DoD Information Resources and Information Technology) and DoDD 8115.01 (Information Technology Portfolio Management).

DoD Component CIOs endorsing the proposed eMASS deployment should acknowledge their support for the requested deployments by sending a signed letter (sample letter available here. A PDF copy of the signed letter can be emailed to an eMASS point of contact (POC), IA51@disa.mil. The letter should include a statement indicating CIO approval for the organization's eMASS use and

should identify an organizational POC for further discussions regarding eMASS procurement and deployment planning.

This endorsement supports information technology portfolio management and is not intended as a substitute for system certification and accreditation authority and processes.

When the approval process is successfully completed, the requesting Command/Service/Agency will be contacted via the POC indicated on the CIO approval letter to begin the planning and coordination process.

7.6 Host Based Security

7.6.1 Host Based Security System (HBSS)

The Defense Information Systems Agency (DISA), at the request of the United States Strategic Command (USSTRATCOM) and in support of National Security goals established by the President, has purchased from industry, a capability that will develop and deploy an automated Host-Based Security System (HBSS) solution(s) that will provide network administrators and security personnel with mechanisms to prevent, detect, track, report, and remediate malicious computer-related activities and incidents across all DoD networks and information systems.

The Host Based Security System (HBSS) baseline is a flexible, commercial off-the-shelf (COTS) based application. The system can detect and counter, in real-time, against known cyber-threats to Department of Defense (DoD) enterprise. Under the sponsorship of the Enterprise-wide Information Assurance and Computer Network Defense Solutions Steering Group (ESSG), the HBSS solution will be attached to each host (server, desktop, and laptop) in DoD. The system will be managed by local administrators and configured to block known-bad traffic using an Intrusion Prevention System (IPS) and host firewall. There is much more to the capabilities of the HBSS system and you can find out more information by reading the material referenced below. DISA is providing program management and supporting the deployment of this solution. The scope of the HBSS deployment is worldwide. This vast effort requires a large support infrastructure to be in place. DISA has instituted support services to enable the comprehensive implementation of the HBSS system to all the CC/S/A and field activities.

- **Standard Features**
  HBSS Standard Features are listed below. The referenced link to each of these features is a product page with links to:

  - Whitepapers
  - FAQ's
  - Lessons Learned

- **Value to Our Mission Partners**
  HBSS can detect and counter against known cyber-threats to Department of Defense (DoD) enterprise in real-time. The HBSS solution is attached to each host (server, desktop, and laptop) within the DoD. The system will be managed by local administrators and configured to block known-bad traffic using an Intrusion Prevention System (IPS) and host firewall. The HBSS solution(s) provide network administrators and security personnel with mechanisms to prevent, detect, track, report, and remediate malicious computer-related activities and incidents across all DoD networks and information systems.

7.6.2 DoD Antivirus Solutions

The DoD antivirus program supports the operation and defense of the Global Information Grid (GIG) by providing virus protection to GIG assets. There are currently two antivirus and anti-spyware solutions available for DoD use: McAfee Virus Scan and Symantec Endpoint Protection.
Both solutions can be standardized and deployed both enterprise-wide and on isolated network enclaves (e.g., a tactical environment) to protect laptops, desktops, servers and e-mail gateways.

❖ **Standard Features**
- Protect assets from SPAM and MALWARE (e.g. viruses, Trojan horses, worms, bots, and rootkits) by filtering e-mail.
- Identify unsafe websites during searches.
- Protects against identity theft by securing, storing, and managing login credentials and personal information.
- Prevents hackers from eavesdropping and stealing information while you type (i.e. keylogging).
- Automatically finds and fixes PC problems while preventing bandwidth.

❖ **Value to Our Mission Partners**

The Antivirus solutions solution(s) provide network administrators and security personnel with mechanisms to prevent, detect, track, report, and remediate malicious computer-related activities and incidents across all DoD networks and information systems.

❖ **Additional Information**

For Additional Information please visit:
http://www.disa.mil/Services/Information-Assurance/Antivirus

7.7 Remediation

Go directly to: https://www.intelink.gov/wiki/Remediation

7.8 Public Key Infrastructure (PKI)

Go directly to: http://iase.disa.mil/pki-pke/

7.9 Cross Domain Solutions

CDES provides support to Combatant Commands, Services, and Agencies by implementing, fielding, and providing lifecycle support for cross domain solution technologies that provide secure interoperable capabilities throughout the Department of Defense. DISA provides consolidated Cross Domain Solutions on behalf of DoD components and develops a robust cross domain fielding capability under the Chairman Joint Chiefs of Staff Instruction (CJCSI) 6211.02C. This is possible by providing net-centric, service-oriented, cross domain information sharing solutions with guaranteed quality of service for authorized users anywhere on the Global Information Grid (GIG). The primary focus is to meet community demands by overcoming varying service guard deficiencies by means of smartly integrating and supplementing critical services without sacrificing security while sustaining performance.

❖ Standard Features
- Standardizes and controls the interfaces to the Cross Domain Enterprise Service cloud that is independent of the guarding technology.
- Improves the fidelity to track, monitor, manage, and report events of customer, guard, and filter usage, including status of operation (i.e. messages, files, and bandwidth processed).

- Provides real-time determination of all customer data flow status and guard availability including individual filters/ flows.
- Provides new boundary applications to enhance security and introduce data processing methods such as web services and performance based high speed data transfer solutions.
- Provides improved insight and situational awareness of the CDES operations and infrastructure to the Network Operations (NETOPS) community.

❖ **Value to Our Mission Partners**
CDES provides net-centric, service-oriented, cross-domain information sharing solutions with guaranteed quality of service for authorized users anywhere on the Global Information Grid.

❖ **Additional Information**
Please visit: http://iase.disa.mil.cds

❖ **Ordering/Price Information**
Please send an email to the CDES Program Manager at: CDES@disa.mil

8 Network Services

8.1 Transport

8.1.1 Dedicated Point- to- Point Service

Dedicated Service is a private-line-transport service that provides point-to-point connectivity to our partner locations. This service supports up to and including TS/SCI security classification.

❖ **Features**
- Ability to carry multiple classifications of traffic
- Small and constant latency per connection
- Efficient utilization of bandwidth
- Wide geographic deployment, which reduces leased-line distances and cost

❖ **Rates/Pricing Information**
Service rate information is located under Inventory and Billing on DISA Direct at https://www.disadirect.disa.mil.

❖ **Additional Information**
The DISN Telecommunications SLA, located on DISA Direct at https://www.disadirect.disa.mil, documents the service performance metrics and management threshold for the DISN telecommunications services that are measured, monitored, and reported.

Our mission partners order DISN telecommunication services via the DDOE application located at https://www.disadirect.disa.mil.

The DGSC serves as the POC for Dedicated Service.

Organization	Contact Information

DGSC	CML: (800) 554-3476 or (614) 692-4790 DSN: (510) 376-3222 or (312) 850-4790
DGSC Email	SBU IP Data Email: DGSC@CSD.DISA.MIL Secret IP Data Email: DGSC@COLS.CSD.DISA.SMIL.MIL

8.2 Data

8.2.1 Sensitive but Unclassified Internet Protocol Data (NIPRNet)

SBU IP Data provides guarded and monitored connectivity to DISA mission partners. This unclassified IP data service for Internet connectivity and information transfer supports DoD applications such as email, web services, and file transfer. The SBU IP Data service also provides DoD mission partners with centralized and protected access to the public Internet. This service supports up to and including SBU security classification.

❖ **Features**

- Connectivity
  - Rate-Limited Access Bandwidth — IP data rate limited to the partner-requested access bandwidth up to the maximum supported by the interface.
  - Control and Routing Exchange — Static configuration or dynamic updates using the BGP that is supported for IP routing between the DISN Edge and CE routers.
- IA Protection
  - Access Load-Sharing and Diversity — Supports multiple access links to improve service survivability. Options for ordering access circuits include load-sharing (active/active) and active primary with secondary backup for interface, node, or site diversity to meet site C2 survivability requirements.
  - External Network Gateways for Perimeter Protection — Provides protected, centralized interfaces to external networks. The internet access points, or gateways, screen DoD network assets from Internet threats and provide secure connectivity to the IC and other federal government and allied networks operating at the unclassified level.
- Network Management
  - Network Time—Network time protocol distributes the time-of-day clock to partner CE routers for system time synchronization and event correlation.

❖ **Value to Our Mission Partners**

The NIPRNET Hardening program is a Defense-in-Depth Information Assurance (IA) and Computer Network Defense (CND) effort designed by DISA to satisfy some, but not all, of the requirements specified by CJCSM 6510.0. The NIPRNet Hardening Program consists of several projects that together will improve the defensive posture of all unclassified DoD networks. The WCF program is one of the associated NIPRNet hardening programs. WCF provides boundary protection at the application layer for web (HTTP/HTTPS) traffic and provides URL filtering for requests and malware filtering on responses. WCF program efforts will assure mission execution in the face of cyber-attack by reducing the NIPRNet attack surface and improving information to attack diagnosis, detection and response (A2DR) systems. The WCF will provide uniform protections for clients against web vulnerabilities. This unclassified IP data service for Internet connectivity and information transfer supports DoD applications such as email, web services, and file transfer. The SBU IP Data service also provides DoD mission partners with centralized and protected access to the public Internet. This service supports up to and including SBU security classification.

In addition, The NIPRNet Federated Gateway (NFG) architecture implements enterprise capabilities that support additional DoD-wide solutions that protect against dangerous protocols, secure DOD-wide Domain Name Service (DNS), and secure enterprise-wide support to the teleworking workforce. This creates a clear boundary between DoD and others; enables improved sharing with key partners; and focuses cyber-attack detection, diagnosis, and reaction on the most important DoD missions. This gives DoD some ability to maneuver at the boundary in response to cyber-attacks. The Secret Internet Protocol Network (SIPRNet) DMZ utilizes a Releasable (REL) and Federal (FED) DMZ to support capabilities for sharing information with coalition partners and United States government agencies. It improves attack detection by providing access control and filtering capabilities; thus decreasing the probability of a successful, adversarial, attack.

❖ **Rates/Pricing Information**

Service rate information is located under Inventory and Billing on DISA Direct at https://www.disadirect.disa.mil.

❖ **Additional Information**

The DISN Telecommunications SLA, located on DISA Direct at https://www.disadirect.disa.mil, documents the service performance metrics and management threshold for the DISN telecommunications services that are measured, monitored, and reported.

Our mission partners order DISN telecommunication services via the DDOE application located at https://www.disadirect.disa.mil.

NOTE: *There are services that require a connection approval. Information regarding connection approvals can be found at http://www.disa.mil/connect.*

The DGSC serves as the POC for SBU IP Data.

Organization	Contact Information
DGSC	CML: (800) 554-3476 or (614) 692-4790 DSN: (510) 376-3222 or (312) 850-4790
DGSC Email	SBU IP Data Email: DGSC@CSD.DISA.MIL Secret IP Data Email: DGSC@COLS.CSD.DISA.SMIL.MIL

8.2.2 Secret IP Data (SIPRNET)

The Secret IP Data provides IP-based secret information transfer across DoD for official DoD business applications such as Email, web services, and file transfer. The Secret IP Data service gateway function provides DoD mission partners with centralized and protected connectivity to federal, IC, and allied information at the secret level. The Secret IP Data service includes IP-based secret information exchange within DoD (DoD intranet) and centralized, gateway external network information exchange (i.e., the extranet). The intranet function provides access to a joint, shared DoD environment at the Secret security classification for the exchange of information among DoD components.

The DGSC serves as the POC for Secret IP Data.

Organization	Contact Information
DGSC	CML: (800) 554-3476 or (614) 692-4790 DSN: (510) 376-3222 or (312) 850-4790

DGSC Email	SBU IP Data Email: DGSC@csd.disa.mil Secret IP Data Email: DGSC@COLS.CSD.DISA.SMIL.MIL

8.2.3 Top Secret/Sensitive Compartmented Information IP Data

The TS/SCI IP Data service is a secure high-speed multimedia communication service between Sensitive Compartmented Information (SCI) users designed to support the DoD Intelligence Information System (DoDIIS) community through the Defense Intelligence Agency (DIA) Regional Support Centers (RSCs). This service supports up to and including TS/SCI security classification.

❖ **Standard Features**

- Quality of Service (QoS) for guaranteed performance of multiple application types
- Multifaceted network management and control capability
- Extends to non-fixed and SATCOM-based sites for tactical users
- Supports voice and video

❖ **Rates/Pricing Information**

Service rate information is located under Inventory and Billing on DISA Direct at https://www.disadirect.disa.mil.

❖ **Additional Information**

Our mission partners order DISN telecommunication services via the DDOE application located at https://www.disadirect.disa.mil.
The DISN Telecommunications SLA located on DISA Direct at "https://www.disadirect.disa.mil" documents the service performance metrics and management threshold for the DISN telecommunications services that are measured, monitored, and reported.

The DGSC serves as the POC for TS/SCI IP Data.

Organization	Contact Information
DGSC	CML: (800) 554-3476 or (614) 692-4790 DSN: (510) 376-3222 or (312) 850-4790
DGSC Email	SBU IP Data Email: DGSC@CSD.DISA.MIL Secret IP Data Email: DGSC@COLS.CSD.DISA.SMIL.MIL

8.2.4 Secret Test and Evaluation Internet Protocol Data

The Secret Test and Evaluation (T&E) IP Data service provides a "test once" operational environment to support a variety of T&E COI. These COIs have the capability to conduct development, certification and operational T&E activities in an operationally relevant T&E environment. This service supports up to and including Secret security classification, as well as, secret releasable classification supporting coalition T&E activities, such as the Combined Federated Laboratory Network (CFBLNet) and JITC coalition interoperability testing.

❖ **Standard Features**

T&E IP transport of cipher-text data supporting T&E enclaves as defined in the Enclave Security Technical Information Guide (STIG).

- Plain-text information exchange not to exceed the secret classification level.

- DISA-managed High Assurance Internet Protocol Encryption (HAIPET) of the cipher-text data for transport across the DISN T&E network.
- IP routing for the Customer Premise Equipment (CPE) data is configured by the user and cipher-text IP packets are routed by the T&E network transport based on routes managed by DISA CONUS, which are configured to provide full-mesh connectivity established among all T&E HAIPET devices and T&E transport routers.
- Support for partner-established VPN/tunnel connection from CPE to
- CPE using Generic Routing

❖ **Optional Features**

- Customer managed cryptographically isolated enclaves
  - Provisioning of CPE connection for Secret T&E IP Data Meet-Me service.
- Site support not to exceed 1,000 man-hours that include end-to-end coordination of implementation service, event support, user/premise equipment installation, circuit provisioning and engineering maintenance, troubleshooting, incidental materials, and related travel.

❖ **Rates/Pricing Information**

Service rate information is located under Inventory and Billing on DISA Direct at https://www.disadirect.disa.mil.

❖ **Additional Information**

Our mission partners order DISN telecommunication services via the DDOE application located at https://www.disadirect.disa.mil.

The DGSC serves as the POC for Secret T&E IP Data.

Organization	Contact Information
DGSC	CML: (800) 554-3476 or (614) 692-4790 DSN: (510) 376-3222 or (312) 850-4790
DGSC Email	SBU IP Data Email: DGSC@csd.disa.mil Secret IP Data Email: DGSC@COLS.CSD.DISA.SMIL.MIL

8.2.5 Secure File Gateway Relay Service

The Secure File Gateway (SFG) Relay Service is a technical solution for ensuring secure data transference between DoD sites and between commercial sites interfacing with the DoD. The resulting solution attempts to address impending DoD security policy changes, the increasing administration workloads as associated with other file transfer services, and the functionality requested by our many partners.

❖ **Standard Features**

- Security
- Administrative Savings
- Partners can configure, update, and manage their own file transfer process or processes
- Email notifications for file receipt, relay success, and relay error results
- Enables simplified scripting capabilities via the partner's relay configuration file
- Provides tools for data encryption, data transformation, and additional security checks
- Entrusts each partner with aggregated relay logs, containing status, resource and security details
- Guarantees data delivery, enables Secure File Transport Protocol (SFTP) checkpoint restarts and provides for data transfer self-healing

- Obtains resolutions from our partners for common errors (e.g. Login failed, Network unreachable, et al)

❖ **Rates/Pricing Information**

Where applicable, to find the Department of Defense (DoD)-approved rates for Cloud Production Systems support, please refer to http://disa.mil/computing/documents/RatesFY12.pdf .

❖ **Additional Information**

DISA has standard performance level data available for our partners to view. Additional data can also be provided as requested. All performance data to be provided will be documented in the Service Level Agreement (SLA) which will be executed when the service is ordered. Additional service and ordering information can be found by emailing or calling the Enterprise Services Directorate (ESD).

Organization	Contact Information
ESD Phone	CML: 303-224-1660 DSN: 926-1660
ESD Email	CSD_SLM@csd.disa.mil

8.3 Voice

8.3.1 Voice over Secure Internet Protocol (VoSIP)

The VoSIP service provides a cost-effective, reliable, and secure means of classified voice communications, secret only, for C2 and non-C2 mission partners with the capability to communicate directly using point-to-point or conference calling. It does provide a media/voice interface (gateway) to the circuit-switched network providing interoperability between the VoSIP service and the Multilevel Secure Voice service. This service supports up to and including Secret security classification.

The process for connecting to VoSIP is defined in the VoSIP/Classified Voice and Video over Internet Protocol Connection Guide (https://www.us.army.mil/suite/doc/23568699).

❖ **Standard Features**

- Voice
  - Provides an interface between the IP Telephony and the circuit-switched network
  - Provides the full range of supplemental user features (e.g., call hold, call transfer, and abbreviated dialing) available from IP telephony
- Security
  - Uses a separate IP address space for voice communications
  - Firewalls are installed at each VoSIP core site and access control lists are deployed on all routers and gateways to ensure that only permitted traffic flows through them
  - Maintains compliance with IA Vulnerability Alert (IAVA) monitoring and implementation according to the guidelines in the IAVA Management Plan
  - The VoSIP services features an identity management solution (IMS) designed to discover, identify and track the use of network resources
- Emergency Access

- Emergency calling based on local policies of each enclave (e.g., Network Operating Center [NOC], Theater Communications Control Center or any other emergency activation capability)
- The Cisco Unified Meeting Place supports emergency access with a host of features (e.g., conferencing features, centralized identity management, access control security mechanisms, host intrusion and detection, directory services, and interoperability with secure voice services)

❖ **Value to Our Mission Partners**

VoSIP provides a permanent and long-term solution for global secure communications among all sites that are part of the VoSIP and secure voice services.

❖ **Rates/Pricing Information**

Service rate information is located under Inventory and Billing on DISA Direct at https://www.disadirect.disa.mil.

❖ **Additional Information**

The DISN Telecommunications SLA located on DISA Direct at "https://www.disadirect.disa.mil" documents the service performance metrics and management threshold for the DISN telecommunications services that are measured, monitored, and reported.

The DGSC serves as the POC for VoSIP.

Organization	Contact Information
DGSC	CML: (800) 554-3476 or (614) 692-4790 DSN: (510) 376-3222 or (312) 850-4790
DGSC Email	SBU IP Data Email: DGSC@csd.disa.mil Secret IP Data Email: DGSC@COLS.CSD.DISA.SMIL.MIL

8.3.2 Sensitive but Unclassified (SBU) Voice (DSN)

SBU Voice provides IP and circuit-switched voice-band data transfer and dial-up videoconferencing. SBU Voice is required to provide assured voice communications to C2 mission partners. Services are provided through the implementation of military unique features, including Assured Service like Multiple Level Precedence and Preemption (MLPP), to support the military C2 functions. This service supports up to and including SBU security classification.

❖ **Standard Features**

- Automated Access – SBU Voice services also provide automated access capabilities to the following networks:
  - International gateways to the defense networks of our allies for cost avoidance of international commercial calling (Australia, Canada, North Atlantic Treaty Organization (NATO), New Zealand, and United Kingdom)
  - EMSS
  - Government Emergency Telephone System (GETS)
- Survivable Service – The following features contribute to the survivability of the SBU Voice:
  - No single point of vulnerability will exist for the entire network

- Transport supporting major installations (base, post, camp, and station, leased or commercial sites/locations) will use physically diverse DISN routes (where possible)

- Assured Connectivity – Special C2 users under the current SBU Voice MLPP scheme (Flash and Flash Override) are provided non-blocking service.
- Interoperable Service – SBU Voice is designed with the capability to permit interconnection and interoperation with similar tactical, U.S. Government, allied, and commercial networks. All hardware and software in the network must be certified as interoperable and IA-accredited as specified.

❖ **Value to Our Mission Partners**

Provides a global inter-base, non-secure, or secure, DoD telecommunications service for Command and Control (C2) use by DoD-authorized users in accordance with national security directives.

❖ **Rates/Pricing Information**

Service rate information is located under Inventory and Billing on DISA Direct at https://www.disadirect.disa.mil.

❖ **Additional Information**

The DISN Telecommunications SLA, located on DISA Direct at https://www.disadirect.disa.mil, documents the service performance metrics and management threshold for the DISN telecommunications services that are measured, monitored, and reported.

Our mission partners order DISN telecommunication services via the DDOE application located at https://www.disadirect.disa.mil.

NOTE: *There are services that require a connection approval. Information regarding connection approvals can be found at http://www.disa.mil/connect.*

The DGSC serves as the POC for SBU Voice.

Organization	Contact Information
DGSC	CML: (800) 554-3476 or (614) 692-4790 DSN: (510) 376-3222 or (312) 850-4790
DGSC Email	SBU IP Data Email: DGSC@csd.disa.mil Secret IP Data Email: DGSC@COLS.CSD.DISA.SMIL.MIL

8.3.3 Top Secret/Sensitive (TS/S) Compartmented Voice

The TS/SCI Voice service provides secure communication between SCI users up to and including TS/SCI security classification. It is designed to support the DoDIIS community through the Defense Intelligence Agency (DIA) Regional Support Centers (RSCs). The service provides global Voice over Internet Protocol (VoIP) communications for DoD within SCI enclaves connected to the TS/SCI IP Data service, and uses stream-based encryption for private voice traffic.

❖ **Standard Features**

- Intelligence Community-wide calling through gateway connectivity to the National Secure Telephone System (NSTS)
- QoS for guaranteed performance of multiple application types
- Multifaceted network management and control capability

- Extends to non-fixed and SATCOM-based sites for tactical users
- Supports data and video

❖ **Rates/Pricing Information**

Service rate information is located under Inventory and Billing on DISA Direct at https://www.disadirect.disa.mil.

❖ **Additional Information**

Our mission partners order DISN telecommunication services via the DDOE application located at https://www.disadirect.disa.mil.

The DISN Telecommunications SLA located on DISA Direct at "https://www.disadirect.disa.mil" documents the service performance metrics and management threshold for the DISN telecommunications services that are measured, monitored, and reported.

The DGSC serves as the POC for TS/SCI Voice.

Organization	Contact Information
DGSC	CML: (800) 554-3476 or (614) 692-4790 DSN: (510) 376-3222 or (312) 850-4790
DGSC Email	SBU IP Data Email: DGSC@csd.disa.mil Secret IP Data Email: DGSC@COLS.CSD.DISA.SMIL.MIL

8.3.4 Multi-level Secure Voice (formerly referred to as "Red Switch")

Provision of this service is in accordance with national security directives in support of Command and Control (C2) and crisis management mission functions. This service supports up to and including Top Secret (TS) security classification.

The Multilevel Secure Voice service includes a range of assured services to C2 users and their missions in an environment of a robust and feature-rich set of capabilities. This service is provided at major C2 facilities (i.e., the National Military Command Center (NMCC) and COCOM headquarters) interconnected through a cryptographically secured network The service is the core of secure voice services during peace time, crisis and time of conventional war by hosting national-level conferencing and connectivity requirements and providing interoperability with both DoD tactical and strategic communities.

❖ **Standard Features**

- High-quality, secure telecommunications for C2 and crisis management
- Extensive, secure voice conferencing capabilities with conference management
- DIA-accredited multilevel security (MLS) capability
- Interoperable service with other networks such as commercial, Voice over Internet Protocol (VoIP), Defense Switched Network (DSN), Voice over Secure Internet Protocol (VoSIP), Joint Worldwide Intelligence Communications System (JWICS), satellite, etc.
- User-dialed secure connections and conferencing to senior DoD civilian and allied decision makers within the secure voice service Communities of Interest (COI) as well as:
  - Flash Override – considered a capability, not a level of precedence. Exercising this capability preempts calls of all other levels or precedence
  - Flash – preempt immediate, priority, and routine calls

- Immediate – preempt priority and routine calls and are reserved for communications pertaining to situations that gravely affect the security of national and allied forces
- Priority – preempt routine calls and are reserved for communications requiring expeditious action by called parties furnishing essential information for conducting government operations
- Routine – routine precedence applies to official government communications that require rapid transmission by telephonic means, but do not require preferential handling. A routine call does not preempt any other call

❖ **Value to Our Mission Partners**

Provides DoD with high quality secure voice telephone and conferencing services for end-to-end use by DoD authorized users.

❖ **Rates/Pricing Information**

Service rate information is located under Inventory and Billing on DISA Direct at https://www.disadirect.disa.mil.

❖ **Additional Information**

The DISN Telecommunications SLA located on DISA Direct at "https://www.disadirect.disa.mil" documents the service performance metrics and management threshold for the DISN telecommunications services that are measured, monitored, and reported.

CJCSI 6215.02C governs the approval authority required for the Multilevel Secure Voice precedence type of service.

Our mission partners order DISN telecommunication services via the DDOE application located at https://www.disadirect.disa.mil.

NOTE: *There are services that require a connection approval. Information regarding connection approvals can be found at http://www.disa.mil/connect.*

The DGSC serves as the POC for Multilevel Secure Voice.

Organization	Contact Information
DGSC	CML: (800) 554-3476 or (614) 692-4790 DSN: (510) 376-3222 or (312) 850-4790
DGSC Email	SBU IP Data Email: DGSC@csd.disa.mil Secret IP Data Email: DGSC@COLS.CSD.DISA.SMIL.MIL

8.4 Video

8.4.1 Dial-up and Dedicated Videoconferencing(DVS-G)

The Dial-up and Dedicated Videoconferencing service is a "meet me" type of service to the DISN Video Service – Global (DVS-G) system and consequently depends on its users to have the appropriate infrastructure to access the system. These services allow simultaneous video and audio communication between two or more videoconferencing facilities (VCFs). The video services include point-to-point and multipoint videoconferencing service between dial-up and dedicated VCFs at unclassified, secret and Allied secret security levels.

A dial-up mission partner can use any of the switched transmission services available (government or commercial).

A dedicated VCF uses a dedicated T1 circuit to connect to the nearest hub.

❖ Standard Features

DISN video service offers the following seven types of conferences:

- Tele-broadcast – Video and audio signals are sent from one VCF to two or more VCFs without a signal being sent in return. This is similar to watching a television broadcast.
- Tele-seminar – Video and audio signals are sent from one VCF to two or more VCFs and only the audio signal is returned. This allows for a fully interactive audio in the conference. This method is often used for distance learning because all participants can see the instructor and hear each other's questions or comments.
- Interactive – Video and audio signals are sent and received by all participants in the conference. This type of DISN Video Services multi-point conference can incorporate one of three different types of switching. Switching refers to the way the control of the conference is handled. DISN Video Service offers four modes of switching.
- Voice Activated – No individual is assigned overall control of the conference and the monitors will change to show the person currently talking.
- Lecture – The lecturer retains control of the conference. The lecturer may allow others to brief but will never relinquish control of the videoconference.
- Chairperson control – The current speaker is in control of the conference. When the current speaker has completed speaking, the speaker selects and passes control to the next speaker(s).

❖ Value to Our Mission Partners

Dial-up and Dedicated Videoconferencing services are available 24 hours a day, 7 days a week, 365 days a year to registered users using fixed, deployed-fixed and mobile resources.

❖ Rates/Pricing Information

Service rate information is located under Inventory and Billing on DISA Direct at: https://www.disadirect.disa.mil.

❖ Additional Information

The DISN Telecommunications SLA, located on DISA Direct at https://www.disadirect.disa.mil, documents the service performance metrics and management threshold for the DISN telecommunications services that are measured, monitored, and reported.

Our mission partners order DISN telecommunication services via the DDOE application located at https://www.disadirect.disa.mil.

NOTE: *There are services that require a connection approval. Information regarding connection approvals can be found at https://www.disadirect.disa.mil.*

The DGSC serves as the POC for Dial-up and Dedicated Videoconferencing.

Organization	Contact Information
DGSC	CML: (800) 554-3476 or (614) 692-4790 DSN: (510) 376-3222 or (312) 850-4790

DGSC Email	SBU IP Data Email: DGSC@csd.disa.mil Secret IP Data Email: DGSC@COLS.CSD.DISA.SMIL.MIL

8.4.2 Top Secret/Sensitive Compartmented Video

The TS/SCI Videoconferencing service provides secure video communication between SCI users and is designed to support the room-based studio quality and desktop conferencing to the DoDIIS community through the DIA RSCs. The service provides global VoIP communications for DoD mission partners within SCI enclaves connected to the TS/SCI IP Data service, and uses stream-based encryption for private video traffic. This service supports security classifications up to, and including, TS/SCI.

❖ **Standard Features**

- Room-based video teleconferencing (VTC) features include the following:
  - High-quality, studio-based videoconferencing
  - Software scheduling assistant
  - Integrated multimedia display capability
  - Desktop VTC features include the following:
  - Ad hoc videoconferencing
  - Integrated directory service

❖ **Rates/Pricing Information**

Service rate information is located under Inventory and Billing on DISA Direct at https://www.disadirect.disa.mil.

❖ **Additional Information**

Our mission partners order DISN telecommunication services via the DDOE application located at https://www.disadirect.disa.mil.

The DGSC serves as the POC for TS/SCI Videoconferencing.

Organization	Contact Information
DGSC	CML: (800) 554-3476 or (614) 692-4790 DSN: (510) 376-3222 or (312) 850-4790
DGSC Email	SBU IP Data Email: DGSC@csd.disa.mil Secret IP Data Email: DGSC@COLS.CSD.DISA.SMIL.MIL

8.5 Wireless

8.5.1 Enhanced Mobile Satellite Services

Enhanced Mobile Satellite Services (EMSS) provides deployed warfighters and partnering agencies with global communications through security and user prioritization enhancements to commercial Mobile Satellite Services (MSS). EMSS includes global handheld voice, data, paging, and sim-less short burst data (SBD) communications and supports up to and including secure security classification.
The service allows real-time access to other EMSS users, the SBU Voice and commercial U.S. and international telephone networks through the Iridium satellite constellation. If those services were unavailable, EMSS mission partners would be able to communicate only with other EMSS mission partners with EMSS handsets.

❖ **Standard Features**

- Secure voice – Encrypts voice communications using National Security Agency (NSA) Type-1 devices at the S and TS level
- Prioritization – Mission Partners can allow or deny access to the service in the event of a national emergency
- Basic Telephony – Mission Partners can place or receive a secure call
- Circuit-Switched Data – Provides Mission Partners with a means of communicating (e.g., transmitting and receiving) high-capacity data with data terminal equipment
- Sim-less SBD Service – Provides a non-circuit-switched high-capacity means of transmitting and receiving packets of data to and from compatible SBD subscriber devices
- Paging Services – Mission Partners can receive numeric or text pages
- Router Unrestricted Digital Information Connectivity Solution (RUDICS)/Apollo – Custom devices in the field may connect to servers on the SBU IP Data and provides no additional service logic beyond a transport pipe by which to transmit partner data

❖ **Value to Our Mission Partners**

EMSS enables the warfighter to communicate with the SBU Voice, Public Switched Telephone Network (PSTN), and SBU IP Data services by leveraging the EMSS gateway that interfaces with those services.

❖ **Rates/Pricing Information**

Service rate information is located under Inventory and Billing on DISA Direct at: https://www.disadirect.disa.mil.

❖ **Additional Information**

The DISN Telecommunications SLA, located on DISA Direct at https://www.disadirect.disa.mil, documents the service performance metrics and management threshold for the DISN telecommunications services that are measured, monitored, and reported.
Our mission partners order DISN telecommunication services via the DDOE application located at https://www.disadirect.disa.mil.

The EMSS Help Desk serves as the POC for EMSS.

Organization	Contact Information
EMSS Help Desk Info	http://www.disa.mil/Services/SATCOM/Comsatcom-Services (301) 225-2251
MSS Ordering Guide	http://www.disa.mil/~/media/Files/DISA/Services/SATCOM/SCO/MSS_Customer_Ordering_Guide.pdf

8.5.2 Secure Mobile Environment Portable Electronic Device

The Secure Mobile Environment-Portable Electronic Device (SME-PED) service provides DoD personnel with wireless mobile communications leveraging continuing investments in intelligence, reconnaissance and C2 capabilities. The service provides personal communication devices with integrated wireless email, Web browsing and document viewing has enabled a new breed of mobile workforce and supports up to and including TS security classification.

❖ **Standard Features**

- Mobile access to classified systems using the SBU IP Data and Secret IP Data services
- Type 1 and non-type 1 encryption for data and voice
- Connection to DoD voice gateway for Multilevel Secure Voice service access
- Connection to the Multiple Commercial Wireless Service for SBU and Secret IP Data services access
- Single entry point for enclaves requiring multiple diverse wireless network services
- Managed end-to-end service with common reliability and security characteristics

❖ **Value to Our Mission Partners**

Provides DoD personnel with unclassified and secret voice and data wireless hand held mobile communications. It is anticipated that the following government organizations will be utilizing SME-PED once FOC in 2012: National Command Authorities, DoD Components, Intelligence Community, and Department of Homeland Security. Starting in 2013, this service offering will be expanded to include support for new handheld mobile devices, applications, and protocols via implementation of a Mobile Virtual Network Operator (MVNO) wireless gateway service. This service will enable DISA to function as the MVNO for the Department, negotiating DoD-wide access contracts with commercial providers resulting in lower cost of ownership for the Warfighter.

❖ **Rates/Pricing Information**

Service rate information is located under Inventory and Billing on DISA Direct at https://www.disadirect.disa.mil.

❖ **Additional Information**

Our mission partners order DISN telecommunication services via the DDOE application located at https://www.disadirect.disa.mil.

The DGSC serves as the POC for SME-PED.

Organization	Contact Information
DGSC	CML: (800) 554-3476 or (614) 692-4790 DSN: (510) 376-3222 or (312) 850-4790

8.6 Satellite

8.6.1 International Maritime Satellite

The International Maritime Satellite (INMARSAT) services utilize a number of different satellite services to provide warfighters with worldwide access and GIG connectivity for diversity, redundancy and availability. The INMARSAT service provides full range of mobile telecommunications airtime services, equipment and maintenance.

❖ **Standard Features**

- Traditional Voice calls, low-level data tracking systems, high-speed internet and data services, distress and safety services
- Mobile Integrated Services Digital Network (ISDN) services used for videophone
- Always-on capability where the users are only charged for the amount of data they send and receive (applicable to Broadband Global Access Network (BGAN) and Mobile Packet Data Service)

❖ **Optional Features**
- BGAN service – simultaneous voice and broadband data communications across most of the world's landmass
- Fleet Broadband – maritime broadband voice and data communications
- Swift Broadband – aeronautical broadband voice and data communications

❖ **Value to Our Mission Partners**

INMARSAT provides warfighters with access to SBU IP Data, Secret IP Network Data, TS/SCI IP Data, SBU Voice and Multilevel Secure Voice to meet their voice and data requirements and supports up to and including TS/SCI security classification.

❖ **Rates/Pricing Information**

For assistance in obtaining INMARSAT pricing, potential partners should submit inquiries to MSS@DISA.MIL.

❖ **Additional Information**

Our mission partners order DISN telecommunication services via the DDOE application located at https://www.disadirect.disa.mil.

The DISN Global Support Center (DGSC) serves as the mission partner POC for INMARSAT.

Organization	Contact Information
DGSC	CML: (800) 554-3476 or (614) 692-4790 DSN: (510) 376-3222 or (312) 850-4790
DGSC Email	SBU IP Data Email: DGSC@CSD.DISA.MIL Secret IP Data Email: DGSC@cols.csd.disa.smil.mil

8.6.2 Commercial Satellite

The Commercial Satellite Service (CSS) utilizes a number of different satellite services to provide warfighters with worldwide access and Global Information Grid (GIG) connectivity for diversity, redundancy and availability. DISA is the only DoD-authorized service provider for commercial fixed satellite services and serves as an advocate for the use of commercial satellite communications (COMSATCOM) in order to increase the availability and flexibility of military communications.
CSS allows for the lease or acquisition of terminals, teleports, landlines, Operations and Maintenance (O&M) support, host-nation support and approvals (i.e., negotiation support services, host-nation approvals, landing rights, frequency clearance, terminal registration, licenses, authorization to operate the terminals), engineering and any other communications resource our partners may require, providing for a true end-to-end, turnkey solution.

❖ **Standard Features**
- Satellite Communications (SATCOM) gateway systems combined with Commercial SATCOM (COMSATCOM) leases allow worldwide access to DISN voice, data, video and transport services
- DoD gateways continually improve GIG connectivity, diversity and redundancy to increase availability and reliability
- IA upgrades protect gateway and partner systems and data

❖ **Value to Our Mission Partners**

Warfighters are provided with access to Sensitive but Unclassified (SBU) Internet Protocol (IP) Data, Secret IP Network Data, Top Secret/Secret Compartmented Information (TS/SCI) IP Data, SBU Voice and Multilevel Secure Voice to meet their voice and data requirements.

❖ Rates/Pricing Information

Service rate information is located under Inventory and Billing on DISA Direct at: https://www.disadirect.disa.mil.

❖ Additional Information

Our mission partners order DISN telecommunication services via the DISA Direct Order Entry (DDOE) application located at https://www.disadirect.disa.mil.

For Commercial Satellite Service, the Global SATCOM Support Center (GSSC) is the single POC service support for all COMSATCOM mission partners. The GSSC operates 24 hours a day, 7 days a week, 365 days a year, and can be contacted as follows:

Organization	Contact Information
GSSC	CML: (719) 554-5531 DSN: (312) 693-5531
GSSC Email	GSSC@ peterson.af.mil
Regional SATCOM Support Center (RSSC)	CML: (813) 828-6845 DSN: (312) 968-6845
RSSC Email	RSSC@macdill.af.mil

9 Spectrum

Access to spectrum enables our warfighter to use many technologies, including radar, navigation, weapons, and communications systems to achieve information dominance and weapons delivery. As a critical and limited resource, spectrum must be managed.

DISA is the Department of Defense (DoD) center of excellence for spectrum management. The mission is to provide strategic spectrum planning, direct combatant command/joint task force support, and enterprise capabilities and services to continually enable effective global spectrum operations for joint warfighters, national level leaders, and coalition partners.

Through its Spectrum Enterprise Services (SES) efforts, DISA, in collaboration with the DoD spectrum community, provides enterprise capabilities and services as well as other transformation initiatives such as deriving a common framework for efficient exchange of data to support interoperability. The Joint Spectrum Center (JSC), a field office within the DSO, provides electromagnetic environment effects (E3) management, training, acquisition support, modeling, information systems, and operations support. Additional details on DSO can be found at http://www.disa.mil/Services/Spectrum/DSO.

9.1 Spectrum-related Applied Engineering

DISA provides tailored engineering support and guidance that enables the DoD and U.S. Military Services to proactively plan, design, acquire, and operate spectrum-dependent systems compatibly in their intended electromagnetic environment. The primary focus is to provide spectrum support to the warfighter.

Recent ongoing projects include conducting analysis and delivering spectrum-related engineering solutions for the following:

- Unmanned Aerial Systems (UAS)
- Low-Observable aircraft
- National Aeronautics and Space Administration Goddard and the Johnson Space Centers spectrum management
- Test and training ranges in Germany and the U.S.
- Ultra-High Frequency Emergency Network , referred to as UEN, for the Pentagon
- Joint Tactical Information Distribution System/Multifunctional Information Distribution System (referred to as JTIDS/MIDS) tactical data systems used by over 30 countries allied with the U.S.
- STARLite tactical reconnaissance radar
- AEGIS Cruiser radars
- Warfighter Information Network - Tactical, referred to as WIN-T.

❖ **Standard Features**

- Spectrum related analysis expertise in all E3 disciplines
- Scenario-based system design and operational effectiveness analysis
- Spectrum certification/host nation supportability
- Completion of comprehensive spectrum supportability (SS) risk assessments, referred to as SSRAs, for new spectrum-dependent systems, which include frequency band studies and cosite/intersite analyses
- Analyses of radiation hazards to personnel, fuels, and ordnance

- Spectrum planning, including analysis of long-term spectrum regulatory implications and global spectrum access
- Engineering support for Requests for Proposals and Source Selection Evaluation Boards, referred to as RFPs and SSEBs respectively.
- Spectrum dependent system baseline performance electromagnetic emission analysis, and radio/radar coverage and propagation effects
- Preparation and review of acquisition documents
- Test and measurement support in the field and in the laboratory
- Assistance in the development of domestic and international spectrum policy for both radars and UAS

❖ Optional Features

In accordance with provisions of the Telecommunications Act of 1996 and DoD guidance, DISA also provides spectrum support to commercial wireless service providers who want to locate their systems on the DoD property. DISA provides definitive E3 analyses to ensure that there will be no adverse impacts to both existing and planned military/DoD system operations.

❖ Value to Our Mission Partners

DISA provides tailored "fee for service" engineering support and guidance to enable the DoD and U.S. Military Services to proactively plan, design, acquire, and operate spectrum-dependent systems compatibly in their intended electromagnetic environment. In addition and in accordance with the provisions of the Telecommunications Act of 1996 and DoD guidance, DISA also provides spectrum support to commercial wireless service providers who want to locate their systems on the DoD property.

❖ Rates/Pricing Information

DISA provides services to DoD Components, non-DoD government agencies, and commercial customers on a cost reimbursable basis.

❖ Additional Information

Additional information is found at http://www.disa.mil/jsc/index.html.

❖ How to Order

Organization	Contact Information
DSO/JSC/OS48 Phone	CML: 410-293-2682/2103 DSN: 281-2682
DSO/JSC/OS48 Email	DSOJSC-J8govt@disa.mil
DSO/JSC/OS48 Mailing Address	ATTN: Applied Engineering Division (OS48) Joint Spectrum Center 2004 Turbot Landing Annapolis, MD 21402-5064
DSO/JSC/OS48 FAX	CML: 410-293-2631 DSN: 281-2631

9.2 Spectrum Technology Testbed Initiative

The Spectrum Technology Testbed Initiative (STTI) testbed is a federation of modeling and simulation (M&S) tools that provides a simulation-based analysis capability to evaluate the operational implications of relocating DoD spectrum dependent systems from the 1710 – 1755 MHz band to other radio frequency (RF) bands authorized for federal use. Operational implications are derived from the M&S of the equipment operating in dynamic operational scenarios, and are measured in terms of statistical distributions of interference levels and communications network performance statistics, such as percentage of lost packets. While the primary goal of the STTI testbed is to support the relocation of displaced systems, the testbed may also be used to evaluate new spectrum management concepts, techniques, and technologies.

The STTI testbed is being developed through a sequence of software releases. It integrates commercial off-the-shelf (COTS) and government off-the-shelf (GOTS) M&S tools with standard models of DoD radio and communications systems and standard operational scenarios. The STTI testbed is designed for simultaneous use by multiple spectrum engineers and spectrum managers. DISA users operate the testbed on behalf of program/product managers to assist them with rapid, efficient creation and execution of complex dynamic simulation models and scenarios, and to provide them with desired outputs and a means to analyze the results.

❖ **Standard Features**

In addition to the inherent features of the federated COTS and GOTS software, the STTI testbed provides the following additional features and capabilities:

- **Scenario Editor Capabilities**
  - Enhanced Satellite Tool Kit scenario editing
  - Import, cull, and edit electromagnetic environment data
  - Integration of enhanced spectrum engineering service algorithms
  - Graphical user interface (GUI) for engineering models
  - GUI for physical layer models
  - Object editing
  - Scenario geo-location editing
  - Object grouping
  - Ability to interchange data and launch complimentary OPNET network models
  - Satellite objects
  - Click and drag trajectory data

- **Engineering Analysis**
  - Dynamic Spectrum Access (DSA) prototype
  - DSA RF interference (RFI) into/from radio system
  - Monte-Carlo and parametric analyses
  - UAS capacity planning
  - Coverage Plots (desired signal level, signal-to-noise ratio, signal-to-interference ratio, and others.)
  - Dynamic RF/networking
  - Multiple Access (MA) self-interference
  - MA RFI into/from radio system
  - Frequency-Distance, Frequency-Angle, & Distance-Angle Curves
  - Required Separation Distance
  - Geo/Non-geostationary satellite RFI into/from radio system

- **Communication and Networking Models**
  - Network protocol building blocks

- Media Access Control layer building blocks
- DoD waveforms
- MA models
- Physical building blocks and Bit Error Rate / Power Spectral Density libraries
- Enhanced propagation models
- Antenna models

- **Radar Models**
  - Search radars
  - Tracking radars
  - Synthetic Aperture Radar (referred to as SAR) radars
  - Deterministic clutter radars
  - Stochastic clutter radars
  - Radar RFI into/from radio systems
  - Radar on radar interference

- **Simulation Engine**
  - STTI Simulation Toolkit, referred to as SST
  - Modular OPNET

❖ **Optional Features (available, but not part of basic service offering).**

❖ Value to Our Mission Partners

Following enactment of the Commercial Spectrum Enhancement Act [Public Law 108-494], and the subsequent auction of the 1710 MHz to 1755 MHz radio frequency band to commercial Advanced Wireless Services, the DoD required tools to support the changes required to make the band available in the shortest possible timeframe. This required development of a testbed capable of simulating the complex electromagnetic environments which DoD systems encounter in actual operational conditions.

The STTI testbed assists program managers of relocating systems with relocation, band sharing strategies, issues related to alternative technical designs, and with quantifying the costs and risks to support relocation-associated decisions. The testbed is also capable of supporting a broader range of studies through the combination of individual M&S application capabilities, JSC databases, and a library of standard model components. These capabilities support general spectrum compatibility studies and simulations that include realistic effects of RF interference on mission performance. In addition, these capabilities support the assessment of spectrum efficiency and the operational impact of new technologies and new spectrum management techniques.

❖ **Rates/Pricing Information**

- Spectrum relocation analyses, for systems being migrated from the 1710-1755 MHz, are funded by the Spectrum Relocation Fund under the provisions of the Commercial Spectrum Enhancement Act. These analyses are provided free of charge to DoD customers.
- Other spectrum analyses which may use the STTI testbed are provided by the JSC Applied Engineering Division (OS48) on a cost reimbursable basis. See Section 9.1 for additional details and ordering information.

❖ **Additional Information**

- Additional information about spectrum relocation can be found on the National Telecommunications and Information Administration (NTIA) website: http://www.ntia.doc.gov/legacy/osmhome/reports/specrelo/index.htm.

- For information about the STTI testbed software, call
- DSO Systems and Technology Branch (OS33) at 410-293-9265 / DSN: 281-9265.

❖ **How to Order**

- The STTI testbed software is not available for sale or distribution.

- DoD customers desiring spectrum analyses using the capabilities of the STTI testbed should contact the Applied Engineering Division. If the analysis pertains to systems formerly located in the 1710-1755 MHz band, please include "Spectrum Relocation" in the title of your request.

Organization	Contact Information
DSO/JSC/OS48 Phone	CML: 410-293-2682/2103 DSN: 281-2682
DSO/JSC/OS48 Email	DSOJSC-J8govt@disa.mil
DSO/JSC/OS48 Mailing Address	ATTN: Applied Engineering Division (OS48) Joint Spectrum Center 2004 Turbot Landing Annapolis, MD 21402-5064
DSO/JSC/OS48 FAX	CML: 410-293-2631 DSN: 281-2631

9.3 Electromagnetic Environmental Effects (E3) and Spectrum Supportability Training and Awareness

DISA provides E3 and SS training and awareness seminars on such topics as electromagnetic compatibility (EMC) design; hazards of electromagnetic radiation to ordnance (HERO), fuel, and personnel; electromagnetic pulse protection; lightning; and grounding, bonding, and shielding through its DoD E3 Program. The DoD E3 Program overall goal is to achieve operational EMC for all electronic and electrical systems, subsystems, and equipment developed, acquired, and operated by the DoD Components. Training and awareness seminars are tailored for various including acquisition, engineering, and spectrum management professionals.

❖ **Standard Features**

- Develops and administers E3 and SS related classroom training and awareness seminars.
- Develops E3 and SS related distance learning modules and other media.

❖ **Optional Features (Available, but not part of basic service offering).**

❖ **Value to Our Mission Partners**

E3 and SS training will provide key skills and understanding for specifying requirements during the acquisitions, test, and evaluation, and recognizing joint operational problems for deployed systems.

❖ **Rates/Pricing Information**

Most services are provided to DoD agencies with no charge to the end user. Most training seminars and media have been approved for unlimited distribution and release to North Atlantic Treaty Organization (NATO) and Combined Communications and Electronics Board nations.

❖ **Additional Information**

Additional details are found at http://www.disa.mil/jsc/index.html .

- Various on-line training modules on E3 , SS, and other spectrum-related topics can be found at Defense Acquisition University website at https://acc.dau.mil

❖ **How to Order**

Organization	Contact Information
DSO/JSC /OS45 Phone	CML: 410-293-HELP(4357) DSN: (312) 281- 4357
Spectrum Operations Support Center (SOSC)	SOSC@disa.mil
DSO/JSC /OS45 Mailing Address	ATTN: E3 Program Support E3 Engineering Division (OS45) Joint Spectrum Center 2004 Turbot Landing Annapolis, MD 21402-5064

9.4 Joint Spectrum Center Ordnance Electromagnetic Environmental Effects Risk Assessment Database

The JSC Ordnance Electromagnetic Environmental Effects Risk Assessment Database (JOERAD) is a software tool that provides the necessary information to manage the conflict between introduced ordnance and RF emitters used in Joint operations.

The complex environment and accelerated tempo of Joint tactical operations demand full situational awareness and capabilities to evaluate risks associated with the RF sensitive ordnance. These ordnance items, if not analyzed, can pose a great threat to personnel and equipment or result in excessive emission controls on essential shipboard equipment. Of all the technology available to the warfighters, JOERAD is a key tool for success in Joint Operations.

❖ **Standard Features**

- Assist in the resolution of potential HERO effects on munitions during the planning of Joint or combined operations or exercises as a pre-deployment planning tool.
- Provides an organic, timely capability to calculate ordnance Safe Separation distances and/or emitter output levels.
- To provide a capability for planners and commanders to plan for or experiment with various real-world scenarios involving the introduction of ordnance, emitters, and units.

❖ **Optional Features (Available, but not part of basic service offering).**

❖ **Value to Our Mission Partners**

JOERAD will enable HERO safe Joint operations by deconflicting potential interactions between ordnance systems and RF emitters.

❖ **Rates/Pricing Information**

JOERAD is provided to DoD agencies with no charge to the end user. JOERAD is not releasable to foreign nations.

❖ Additional Information

For additional information on JOERAD, access http://www.disa.mil/jsc/index.html

❖ How to Order

Organization	Contact Information
DSO/JSC/OS45 Phone	CML: 410-293-HELP(4357) DSN: (312) 281 - 4357
SOSC Email	SOSC@disa.mil
DSO/JSC/OS45 Mailing Address	ATTN: Ordnance E3 Program E3 Engineering Division (OS45) Joint Spectrum Center 2004 Turbot Landing Annapolis, MD 21402-5064

9.5 SPECTRUM XXI

SPECTRUM XXI is a client/server, Window-based software system that provides frequency managers with a single information system to address spectrum management automation requirements. SPECTRUM XXI supports operational planning and management of the RF spectrum with an emphasis on assigning compatible frequencies and performing spectrum engineering tasks. SPECTRUM XXI is the Joint standard system for spectrum management throughout the DoD. It has also been adopted by the NTIA for processing frequency records for Federal agencies. SPECTRUM XXI was also provided to over 22 foreign nations through Foreign Military Sales (FMS) and these efforts have paid off with SPECTRUM XXI being used by all NATO International Security Assistance Forces spectrum management elements in the Afghan Area of Operations. The DSO Systems and Technology Branch (OS33) is the SPECTRUM XXI office of primary responsibility (OPR).

❖ Standard Features

- Frequency Assignment – automates the processing of request for the use of frequency resources from spectrum managers in support of authorized users. The process includes preparation and validation of frequency assignment proposals, determination of interference with the background environment, and distribution and tracking of proposals.
- Allotment Plan Generator – creates a list of frequencies referred to as allotment plans or channelization plans. These plans are used as frequency resources for nominating proposals using the Frequency Assignment feature.
- Interference Analysis – analyzes existing frequency assignments for potential interference.
- Interference Report – generates a report to describe an interference problem and to provide information that can be used to resolve the problem.
- Topographic Manager –automatically reformats Digital Terrain Elevation Data from the National Geospatial-Intelligence Agency (NGA) for use by the engineering algorithms within SPECTRUM XXI.
- Compliance Validation- checks for compliance of frequency records with the Frequency Allocation Tables, the NTIA Manual, and the coordination requirements with Canada and Mexico.

- Engineering Tools – collection of utilities to perform various types of analyses such as coverage and cosite analysis.
- Electronic Warfare (EW) Deconfliction - assesses the impact of a planned electronic attack (jamming) on existing receivers during contingency operations and exercises.
- Joint Restricted Frequency List – management tool used by various operational and support elements to identify the level of protection they desire to be applied to specific spectrum assets (i.e. frequencies or frequency bands) in order to preclude these assets from being "jammed" by friendly forces conducting EW activities.

❖ **Optional Features (Available, but not part of basic service offering).**

❖ **Value to Our Mission Partners**

SPECTRUM XXI addresses the automated spectrum management requirements processes of the Combatant Commands, Joint Task Force, Services, and the sustaining-base elements. The resulting benefit is interference-free frequencies for the battlefield use while also ensuring that coordination of frequency assignments through national and host nation approval continues.

❖ **Rates/Pricing Information**

SPECTRUM XXI system is available at no cost to U.S. government customers. SPECTRUM XXI server and client software, along with technical support, is also available to US Allies via the FMS process.

❖ **Additional Information**

No service-level agreement (SLA) is required.

❖ **How to Order**

Organization	Contact Information
SPECTRUM XXI Hotline Phone	CML: (410) 293-7994 DSN: 312-281-7994 Manned 0800-1700 Eastern Standard Time or 1400-2300 GMT
SPECTRUM XXI Hotline Email	SOSC@disa.mil
SPECTRUM XXI Hotline Mailing Address	Spectrum Operations Support Center (SOSC) 2004 Turbot Landing Annapolis, MD 21402-5064
DSO/OS33 Mailing Address	ATTN: SPECTRUM XXI OPR DSO Systems and Technology Branch (OS33) Joint Spectrum Center 2004 Turbot Landing Annapolis, MD 21402-5064

9.6 Global Electromagnetic Spectrum Information System - Host Nation Spectrum Worldwide Database Online

The Global Electromagnetic Spectrum Information System (GEMSIS) is the Joint program of record that is transforming spectrum operations from a pre-planned and static frequency assignment process into a dynamic, responsive, and agile capability. GEMSIS will provide a secure and globally connected suite of spectrum management services and deliver capabilities through an evolutionary incremental acquisition approach where each successive increment will build on the previous increment to further mature the GEMSIS architecture with more capabilities and interfaces.

The current GEMSIS baseline includes Host Nation Spectrum Worldwide Database Online (HNSWDO), a web application that provides worldwide visibility of host nation RF spectrum dependent equipment's supportability. It automates distribution of Host Nation Coordination Requests (HNCRs) and combatant command submission of host nation supportability comments, reducing the time required to manage the process, enabling managers to determine the historical supportability of similar systems' RF spectrum. This provides informed design decision-making concerning frequency bands, thereby mitigating the risk of acquiring potentially unsupportable RF dependent systems. HNSWDO operates on the GIG from a server that resides on the NIPRNET, with an equivalent server on the SIPRNET to allow for coordination of classified content. HNSWDO is accessible through these two networks via a user's local web browser, enabling coordination with all relevant coalition partners without them having to install an application on their computer.

❖ Standard Features

GEMSIS (HNSWDO) provides spectrum management services to assess SS, which include:

- Prepare DoD HNCRs.
- Facilitate distribution of DoD HNCRs and combatant command submission of host nation supportability comments.
- Determine historical supportability of other (or similar) systems in the same frequency band.

❖ Optional Features (Available, but not part of basic service offering).

❖ Value to Our Mission Partners

GEMSIS (HNSWDO) aids acquisition programs in controlling risks for spectrum dependent systems being deployed overseas.

❖ Rates/Pricing Information

There is no cost for DoD Components. Foreign sales and commercial access outside the bounds of DoD support activities will be addressed on an individual basis.

❖ Additional Information

GEMSIS (HNSWDO) does not require a SLA with customers for use of its services. Additional system access requirements can be obtained from the helpdesk or web site shown below.

❖ How to Order

Organization	Contact Information
GEMSIS (HNSWDO) Phone	CML: 410-293-HELP(4357) DSN: (312) 281-HELP
GEMSIS (HNSWDO)	HNSWDO@disa.mil

Email	HNSWDO@disa.smil.mil
GEMSIS (HNSWDO) Web Site	https://hnswdo.jsc.mil
DSO/OS31 Mailing Address	ATTN: GEMSIS OPR DSO Systems Engineering Branch (OS31) Joint Spectrum Center 2004 Turbot Landing Annapolis, MD 21402-5064

9.7 Joint Spectrum Data Repository

The DSO has been chartered to collect, standardize, and distribute spectrum-related data. To fulfill this mission, the DSO provides direct on-line data access to the Joint Spectrum Data Repository (JSDR) or provides customized reports. The JSDR contains DoD, national, and international spectrum-related information up to the Secret level and can be accessed via the JSC Data Access Web Server (JDAWS) tool. JDAWS provides user access to the database components of JSDR except Equipment Location-Certification Information Database (EL-CID).

❖ **Standard Feature**

The JSDR features the following spectrum-related databases:

- Joint Equipment, Tactical and Space (JETS) Database - The JETS segment of JSDR is a DSO created and maintained resource that includes: Parametric data for DoD; commercial and coalition equipment (JETS-E); Platform data, including equipment complements (JETS-T); US military unit names, locations and hierarchy (JETS-T); US military unit equipment and platform complements (JETS-T); and space satellite parametric and orbital data (JETS-S).
- (EL-CID) - This master Oracle database contains approximately 25 EL-CID certifications approved by NTIA.
- HNSWDO - This database is a web-based application for processing DoD HNCRS and responses.
- Spectrum Certification System (SCS) Database – SCS is the central archive repository for all DoD Spectrum certification system data, including information from the J/F-12 Application for Equipment Frequency Allocation.
- Background Environmental Information (BEI) Database - To accurately represent the electromagnetic environment, the DSO also collects additional non-U.S. Federal and international frequency assignments, which are stored in the BEI database. The BEI currently includes International Telecommunications Union (referred to as ITU), Federal Communications Commission, Canadian, and Radio Astronomy assignments.
- Government Master File (GMF) Database – This data source contains records of the frequency assigned to all U.S. Federal Government agencies in the U.S. and its possession. Data is obtained from NTIA.
- Frequency Resource Record System (FRRS) Database – FRRS contains information on DoD frequency assignments used throughout the world that is controlled by the Commanders of the Unified Commands and the Military Departments.
- Electronic Order of Battle (EOB) database – The JSDR contains nearly 25,000 Defense Intelligence Agency EOB foreign equipment locations.

- Area Studies - A collection of over 100 DSO-produced country-specific telecommunication profiles is hosted on Intelink. JDAWS capability provides a list of all area studies with hyper-link access to the Intelink site.

❖ **Optional Features (Available, but not part of basic service offering).**

❖ Value to Our Mission Partners

The JSDR provides DoD and its mission partners with direct online access to comprehensive, relevant, accurate, and trusted spectrum data, used to characterize spectrum-dependent systems characteristics and define the electromagnetic environment.

❖ **Rates/Pricing Information**

The DSO provides access to the JSDR with no cost to the end user.

❖ **Additional Information**

None

❖ **How to Order**

Organization	Contact Information
SOSC Phone	CML: 410-293-HELP(4357) DSN: (312) 281-HELP
SOSC Email	SOSC@disa.mil
DSO/OS32 Mailing Address	ATTN: JSDR OPR DSO Data Branch (OS32) Joint Spectrum Center 2004 Turbot Landing Annapolis, MD 21402-5064

10 Testing Services

10.1 Joint Interoperability Test Command

The Joint Interoperability Test Command (JITC) professionally tests, operationally evaluates, and certifies IT capabilities for joint interoperability, enabling information dominance and increasing warfighter effectiveness for the Nation.

❖ **Additional Information**
If you need program or system support, please obtain a General Testing Support Form. For general test support, provide the requested info and an Action Officer will contact you within two working days. Or you may prefer to contact us by phone at **703-882-2280** / **301-744-2804**.

10.2 System Tracking Program (STP)

The System Tracking Program (STP) is an on-line database that tracks a system's progress toward joint interoperability certification. The STP monitors the complete life-cycle of Information Technology (IT) and National Security Systems (NSS) from requirements/capabilities document status, to Interim Certificate to Operate (ICTO), through test and evaluation, and culminating with joint interoperability certification status.

❖ **Additional Information**
To Access the STP, please visit: https://stp.fhu.disa.mil, and complete the following steps:

1. Click on **Apply for STP User Account**.
2. Fill out the form completely, and then press the **Submit Request** button.
3. A username and password will be assigned after designated approval authorities at the JITC review the application. Turnaround time is approximately two workdays.
4. You will then receive an email informing you if your request has been approved or denied.

Please note that the NIPRNET STP is available to .MIL or .GOV domain users only. Contractors applying for STP access must have a government sponsor and a need to know.

10.3 Joint Interoperability Tool (JIT)

The JITC Joint Interoperability Tool (JIT) provides high speed access to key interoperability information. The heart of the system is an extensive data repository featuring the JITC Lessons Learned Reports, JITC Test Reports, the NATO Interface Guide, Joint Interoperability Certification Letters, and other interoperability documents and references; as well as a high speed search engine to quickly access data. This tool gives a quick and easy on-line capability which identifies system/equipment characteristics, tested configurations and practical "how-to" information to facilitate interoperability.

❖ **Standard Features**
To see the features and capabilities of the JIT please go to: http://jitc.fhu.disa.mil/brochure/jit.pdf

❖ **How to Access the JIT**
To access the JIT you will require access to either a NIPRNet/Internet or SIPRNet workstation and a web browser.

❖ **Additional Information**

IMPORTANT: The JIT requires the use of a DoD-issued Identification Certificate to gain access to the website. An Identification Certificate issued by a DoD-approved External Certificate Authority is also acceptable. When asked to verify certificate, be sure to select your Non-email certificate.
If you need program or system support, please obtain a General Testing Support Form. For general test support, provide the requested info and an Action Officer will contact you within two working days. Or you may prefer to contact us by phone at 703-882-2280 / 301-744-2804.

10.4 Testing / Interoperability Certification

DISA, through its Joint Interoperability Test Command (JITC) field element, can provide its users different types of test services ranging from standards conformance (developmental or verification testing) to full capability (operational) testing.

JITC provides testing expertise to its Department of Defense (DoD) and non-DoD customers through its three unique roles:

- Joint Interoperability Certifier. As programs advance through the DoD acquisition lifecycle, they must meet certain criteria in order to successfully address their developmental milestones. For Information Technology (IT) and National Security Systems (NSS), one of those criteria is to obtain an interoperability certification from JITC. By Federal mandate, JITC is the only Agency that certifies DoD IT and NSS meet interoperability requirements for joint military operations.
- Operational Test Agency. In its role as a DoD Joint Operational Test Agency (OTA), JITC conducts operational testing of IT and NSS under realistic conditions, to determine the operational effectiveness, suitability, interoperability, and security of a particular system, and independently assess the operational impact of system issues on mission accomplishment.
- Warfighter and Coalition Interoperability Support. JITC works closely with the warfighting combatant commanders during exercises and contingency operations to provide them on-the-spot evaluations of problem areas and realistic solutions.

❖ **Standard Features**

JITC testing includes the following services:

- Early participation in requirements development and developmental tests to provide operational insights to Program Managers and decision-makers.
- Agile methods for data collection, reduction, analysis, and reporting to reduce the acquisition and testing cycle times.
- Integrated test approaches to maximize information reuse and minimize test redundancies.
- Maximum use of training and exercise activities to increase the realism and scope of testing and to reduce testing costs.
- Testing Net-Centric and Web-based applications at both system and enterprise level.

❖ **Optional Features**

- Technical support hotline. This 24/7/365 day, no cost to the customer, service provides prompt support to the warfighters—whether you're a private in a foxhole or the Commander. JITC has an extensive level of expertise and experience as well as a tremendous capability to recreate most any equipment string in an effort to duplicate interoperability problems to find potential solutions. Hotline calls are treated as either "Critical" or "Routine".
    - For users who are currently deployed, or in support of on-going exercise/contingency operations, their requests are treated as critical and a Hotline representative will respond to their request within two hours.

- All other requests are considered routine, and a Hotline representative will respond by the next business day.

❖ Rates/Pricing Information

JITC is the only non-Service and IT-focused element of the DoD Major Range and Test Facility Base (MRTFB). The MRTFB is a national asset which is sized, operated, and maintained primarily for DoD test and evaluation support missions. The DoD Financial Management Regulation (FMR) 7000.14-R prescribes the charge policy for MRTFB facilities.

JITC charges its reimbursable customers all direct costs, such as Government and contract labor, equipment, supplies, items damaged or used during testing, etc., that are identified to a specific customer. Non-DoD customers also pay a portion of JITC's indirect costs, which include the costs of maintaining, operating, upgrading, and modernizing JITC and its laboratories.

To see the DoD-approved rates charged to reimbursable customers, please refer to:

- DoD FMR, http://www.defenselink.mil/comptroller/fmr/
- U.S. Office of Personnel Management (OPM) Salary Tables: http://www.opm.gov/oca/payrates/index.asp

❖ Additional Information

JITC provides extensive test-related services to address their customers' unique testing and test information needs. These include:

- DoD Interoperability Communications Exercise (DICE). JITC hosts tri-annual DICE events that provide an agile testing environment to quickly get systems to the battlefield. DICE provides:
  - Live and closed networks to enable systems testing at various stages of development.
  - Automated tools and distributed testing.
  - Connectivity to a representative Joint Task Force communications architecture.
  - Technical Subject Matter Experts.
  - Realistic testing without operational pressures.
  - Resource sharing leading to cost-effective testing.

- DoD Approved Products List (APL). JITC maintains the DoD APL, which is the only listing of equipment to be fielded in DoD networks. DoD components are required to purchase APL listed products, if one of the listed products meets their needs. If no listed product meets the organization's needs, they may sponsor a product for testing. For more information or to view the APL, please refer to https://aplits.disa.mil.

- JITC's Joint Interoperability Tool (JIT). The JIT provides high speed access to key interoperability information. The heart of the system is an extensive data repository featuring the JITC Lessons Learned Reports, JITC Test Reports, the NATO Interface Guide, Joint Interoperability Certification Letters, and other interoperability documents and references; as well as a high speed search engine to quickly access data. This tool gives a quick and easy on-line capability which identifies system/equipment characteristics, tested configurations and practical "how-to" information to facilitate interoperability. For more information or to request access to the JIT, please refer to https://jit.fhu.disa.mil.

- The System Tracking Program (STP). JITC's STP is an on-line database that tracks a system's progress toward joint interoperability certification. The STP monitors the complete life-cycle of Information Technology (IT) and National Security Systems (NSS) from requirements/capabilities document status, to Interim Certificate to Operate (ICTO), through test and evaluation, and culminating with joint interoperability certification status. For more information or to request access to the STP, please refer to https://stp.fhu.disa.mil.

- JITC Lessons Learned Reports. JITC's Lessons Learned Reports are designed to provide the user in the field with information not readily available through conventional sources such as Technical Manuals, Technical Orders, and other official documentation. The primary target audiences for the reports are the equipment operators/maintainers and system planners. For more information or to access JITC's Lessons Learned Reports, please refer to https://jit.fhu.disa.mil/llr/.

❖ How to Order

Additional service and ordering information:

Organization	Contact Information
JITC Phone/Hotline	CML: 1-800-LET-JITC (538-5482) DSN: TRY-JITC (879-5482)
JITC Email	JITCsupport@disa.mil

11 Pipeline Services (New Services in Development)

DISA's long term vision is to provide a true communications and collaboration service that can be leveraged as enterprise services. Unified Communications and Collaboration (UC&C), is the integration of synchronous communication services (e.g., web conferencing, Instant Messaging (IM)/chat, voice telephony, video conferencing, etc.) with asynchronous communication services such as unified messaging, portals, and other applications. UC&C can be a product suite offered by one vendor or a set of integrated products that provides a unified user interface and user experience across multiple devices and media types. The following services / systems are in various stages of planning and development for inclusion into the DISA Service Catalog. Some are designed as Enterprise offerings, others are based on Military Service/Defense Agency requirements. We will move these services forward in this document and add additional information as the service nears production.
Please direct any questions about pipeline services to one of the following:

- DISASERVICECATALOG@csd.disa.mil
- CSD_SLM@csd.disa.mil
- 303-224-1768

11.1 National Senior Leader Decision Support System (NSLDSS)

NSLDSS will provide web-based, thin client capabilities in order to provide accurate, timely, and focused situational awareness of situations, operations, and events of interest around the world; enable collaborative development, presentation, assessment, and selection of COA options to respond to some event or situation of concern; support collaborative decision-making during national conferences; and deliver key data to senior leaders regardless of their physical location and display device, as long as they have access to the correct network. It leverages enterprise services, exposes data to the enterprise as a service, uses an adaptable, layered architecture and facilitates trust by using authoritative data sources.

The following capabilities will be provided as part of the NSLDSS service:

- **Universal Description Discovery and Integration (UDDI)** – A platform-independent, Extensible Markup Language (XML)-based registry for DoD mission partners allowing them to list themselves and a mechanism to register and locate available web service applications. It will allow discovery, interaction, and communication technology to join disparate systems and information providers. It is a self-contained business function that operates over the internet to support program-to-program interactions. This web service will be integrated with DISA's service oriented architecture.
- **Joint User Messaging (JUM)** – JUM is a secure, reliable, message delivery functionality supporting: Machine-to-Machine (M2M) messaging via SOAP web services; User-to-User messaging via web browser; and User-to-Machine messaging using message templates. It provides a secure infrastructure for subscribing and publishing to information topics in real time. It can reliably share data with multiple authorized consumers without the technical and operational problems associated with maintaining a large number of point-to-point system interfaces. JUM users and capabilities will be absorbed into Enterprise Messaging by fall of 2012.
- **Joint Enterprise Directory Service (JEDS)** – JEDS is an enterprise-wide directory service that provides DoD People Discovery (i.e. white pages) and DoD identity management attributes services to support DoD access control decisions. DISA established the JEDS initiative to provide the DoD with this identity information-sharing functionality. JEDS harvests and correlates data from multiple DoD data sources that contain pertinent information about DoD people, objects, and

resources and makes it available to DoD users through a central public key infrastructure (PKI) enabled site. The JEDS currently provides a DoD-wide search functionality for information (names, contact information, and other job related attributes) regarding DoD personnel on both the NIPRNet and SIPRNet. JEDS will be sunset and its functionality enveloped into the Enterprise Application and Services Forest (EASF).

11.2 Enterprise Messaging (EM)

EM is a web service that will allow applications to publish and receive information such as special reports, alerts, briefs, or section-specific information over specialized logical messaging channels. It supports the configuration of Quality of Service (QoS) for a published message, including the priority, precedence, and time-to-live. EM provides a federated, distributed and fault-tolerant message bus. It delivers high performance, scalable, and interoperable synchronous (pull) and asynchronous (push) event notifications to applications using publish and subscribe messaging. It provides guaranteed delivery to disconnected users or applications, and uses multiple message brokers, potentially within different administrative domains, to support the distributed, federated nature of the enterprise. EM will achieve IOC by summer of 2012. Users on Joint User Messaging (JUM) and Machine to Machine-NCES Messaging (WS_Enventing) will be seamlessly, rolled into EM by fall of 2012.

11.3 Testing as a Service (TaaS)

This offering will complement existing services/programs (RACE, Forge.mil, DTEN) by tying testing components together along with other independent initiatives currently underway at DISA into a single Testing Service. TaaS will determine the metrics for Enterprise Solutions in the areas of Suitability, Performance, and Interoperability. It will define new enterprise test methods and access external data sources to use as certification tools. Primarily, TaaS will identify the certification requirements for any product that will be tested in the Enterprise environment. Standard specifications for interoperability, security, performance or anything else governed by a standard or instruction will have business rules established to automatically assign requirements. This means that owners of this functionality will receive a checklist to develop to, and when the product is ready, the owner can conduct self-certifications, store results, and request JITC or the DAA to evaluate the results for formal certification. Testing as a Service is currently in the middle of its design phase and is planned to have a completed design within the beginning months of calendar year 2012. TaaS will have a pilot complete by mid-2012 and is scheduled to achieve Initial Operational Capability (IOC) by the end of 2012.

11.4 DoD Storefront

Provides a compelling, flexible web-based platform on which to build and share applications and information services with DoD users. This will be a robust Web 2.0 widget framework and an application marketplace to foster rapid development, sharing, and use of DoD capabilities and enable the use to tailor the experience to meet their specific needs.

11.5 Future Mission Network (FMN)

FMN is a service that enables senior leaders and Commanders at all levels the ability to establish Command and Control (C2) and operations on little to no notice. Users will have the ability to execute US unilateral or coalition operations across the spectrum of conflict, humanitarian aid, and disaster relief from 'Day 1 of Phase 1' until 'Mission Complete'. Currently, FMN is in the development phase and will be integrated into DISA's Joint Enterprise Services to ensure readiness and responsiveness to the requirements of Combatant Commanders.

12 Service Support and Assistance

DISA has deployed several support organizations that specialize in assisting our Partners understand and obtain DISA services. Some are based on types of service being provided, others are based on the Military Service/Defense Agency being supported and some are a hybrid of both. These supplement and are in addition to the many Points of Contact included in this Service Catalog.

12.1 For Support Using this Service Catalog

If there are questions that concern how to use this catalog or that requires amplification of the information contained therein or obtaining information not found in this catalog, please contact the Catalog Manager at:

(303) 224-1768, DSN 926
DISASERVICECATALOG@disa.mil

12.2 DISA Command Center (DCC)

The DISA Command Center (DCC) exercises the authority and direction of the DISA director over assigned and attached DISA network operations (NetOps) forces in the execution of the cyber mission. The DCC provides the command and control capability for the DISA director along with situational awareness of the agency's provided infrastructure, computing, and enterprise services. The center directs DISA's worldwide operations and exercises operational control over DISA NetOps, computing centers, DISA field offices, and other operational organizations. It ensures continued quality customer service to all of DISA's global customers.

(301) 225-3507, DSN 375
DISA-DCC-CENTRAL@DISA.MIL

12.3 DISA Joint Staff Support Center (JSSC)

The JSSC provides leading edge capabilities for Command and Control, Information Assurance, Multimedia, Web Risk Assessment, and Continuity of Operations to warfighters, National level leaders, and other mission partners. The JSSC is renowned for providing agile world class C4I capabilities to the warfighter.

(703) 695-0671, DSN 225
http://www.disa.mil/About/Our-Organization-Structure/OD-Field-Office/Joint-Staff-Support-Center

12.4 DISA Field Security Operations

Responsible for enhancing security and availability of the Global Information Grid by ensuring adherence to Information Assurance and NetOps Policies including development of guides and procedures; training of DoD, DISA, and Combatant Commands; implementation of Enterprise IA solutions; formal certification reviews; vulnerability management tools and metrics; NetOps training and reviews; CNDSP, NetDefense, Incident Response; and Enhanced Compliance Validation inspections.

(717) 267-9876, DSN 570
FSO_SLM@disa.mil
http://www.disa.mil/About/Our-Organization-Structure/OD-Field-Office/Field-Security-Operations

12.5 DISN Global Support Center (DGSC)

The DISN Global Support Center (DGSC) is the single point of contact for our mission partners providing 24/7 support. The DGSC is an industry certified support center and is responsible for making an initial assessment of the contact and attempt first contact resolution (FCR), escalating and tracking all other contacts, closing resolved contacts, logging service requests, executing the transactional surveys, and managing service desk key performance indicators to meet customer expectations.
The DISN Global Support Center (DGSC) is available twenty four hours a day to assist DISN mission customers with questions, escalations, or support issues not related to outages.

DSN: (510) 376-3222 or (312) 850-4790
CML: (800) 554-3476 or (614) 692-4790
DGSC@CSD.DISA.MIL

12.6 COCOM-Dedicated Field Support Offices

To fully optimize mission-partner engagement to the Combatant Commands (COCOM), DISA has established Field Support Offices (FSO) co-located with and dedicated to the COCOMs. The mission of the FSOs is to be the combat support agency's forward representative to the COCOMs responsible for providing direct support for net-centric solutions across the Global Information Grid in the COCOM operational mission areas of responsibility. Additional information about the FSOs and how to utilize their capabilities can be obtained from the following:

- **DISA African Command (DISA AFRICOM)**
  - **Vaihingen, (Stuttgart) GE**
  - **(0711) 729-4521, DSN (314) 421-4521**
  - http://www.disa.mil/About/Our-Organization-Structure/OD-Field-Office/AFRICOM
- **DISA Central Command (DISA CENT)**
  - **MacDill AFB, FL**
  - **(813) 827-6403, DSN 651**
  - http://www.disa.mil/About/Our-Organization-Structure/OD-Field-Office/CENT
- **DISA Continental United States Command (DISA CONUS)**
  - **Scott AFB, IL**
  - **(618) 229-8840/8801, DSN 779**
  - http://www.disa.mil/About/Our-Organization-Structure/OD-Field-Office/Field-Office-Directory
- **DISA Europe Field Command (DISA Europe)**
  - **Vaihingen, (Stuttgart) GE**
  - **DSN (314) 434-5190**
  - http://www.disa.mil/About/Our-Organization-Structure/OD-Field-Office/EUROPE
- **DISA US Joint Forces Command (DISA JFCOM)**
  - **Norfolk, VA**
  - **DSN 836-5753**
  - http://www.disa.mil/About/Our-Organization-Structure/OD-Field-Office/JFCOM
- **DISA Northern Command (DISA NORTHCOM)**
  - **Peterson AFB, CO**
  - **(719) 554-3800 / 5962, DSN 692**
  - http://www.disa.mil/About/Our-Organization-Structure/OD-Field-Office/NORTHCOM
- **DISA Pacific Command (DISA Pacific)**
  - **Ford Island, HI**

- **(808) 472-0051, (315) 472-0051**
- http://www.disa.mil/About/Our-Organization-Structure/OD-Field-Office/PACIFIC

❖ **DISA Special Operations Command (DISA SOCOM)**

- **MacDill AFB, FL**
- **(813) 826-2086, DSN 299**
- http://www.disa.mil/About/Our-Organization-Structure/OD-Field-Office/SOCOM

❖ **DISA Southern Command (DISA SOUTHCOM)**

- **Miami, FL**
- **(305) 437-1671, DSN 567**
- http://www.disa.mil/About/Our-Organization-Structure/OD-Field-Office/SOUTHCOM

❖ **DISA Strategic Command (DISA STRATCOM)**

- **Offutt AFB, NE**
- **(402) 294-5761, DSN 271**
- http://www.disa.mil/About/Our-Organization-Structure/OD-Field-Office/STRATCOM

❖ **DISA Transportation Command (DISA TRANSCOM)**

- **Scott AFB, IL**
- **(618) 229-1841**
- http://www.disa.mil/About/Our-Organization-Structure/OD-Field-Office/TRANSCOM

12.7 Enterprise Services Directorate (ESD) Partner Relations Management

DISA ESD is charged with the provision of enterprise services, enterprise applications, all computing services, the Rapid Access Computing Environment (RACE) testing service, the Global Content Delivery Service (GCDS), various other business applications and management of the DECCs To better enable our partners to utilize these services, ESD has established Partner Relations Management Teams that provide one place to obtain answers on all ESD services and capabilities. These Teams feature dedicated, multi-skilled professionals dedicated to each Military Service and Defense Agency. Team staffs consist of information technology technicians, project managers, account representatives and systems and software engineers. Included in the responsibilities of this division are:

- Creation and maintenance of Service Level Agreements (SLAs).
- Preparation of engineering designs and business proposals for new partner workload.
- Project management of new workload implementations.
- Handling all issues and questions identified by our partners.
- Joining with our partners to develop strategies that achieve cost savings and efficiencies.

These teams are structured as follows:

❖ **Air Force Support Team**
(301) 225-7009, DSN 375

❖ **Army Support Team**
(301)225-7214, DSN 375

❖ **DFAS/DLA/TRANSCOM Support Team**
(717) 605-5280, DSN 430

- **DISA Support Team**
  (301)225-7012, DSN 375

- **Joint Staff/COCOM/OSD/DoD & Classified Support Team**
  (301)225-7228, DSN 375

- **MHS/TRICARE Support Team**
  (334)416-5894, DSN 596

- **Navy/Marine Corps Support Team**
  (717)605-6720, DSN 430

- **ESD Hotline**
  (303)224-1660, DSN 926
  CSD_SLM@csd.disa.mil

12.8 DISA Defense Enterprise Computing Center (DECC) Service Desk Contact Information

- **DECC Chambersburg**
  - **717-267-5690, DSN 570-5690**
  - ChambersburgProcessingElement@csd.disa.mil
- **DECC Columbus**
  - **800-554-3476, DSN 850-1710**
  - SMCDESK5@csd.disa.mil
- **DECC Dayton**
  - **937-257-3251, DSN 787-3251**
  - DISAPEDDaytonCivilian@csd.disa.mil
- **DECC Europe**
  - **+49(0)711-68639-5067, DSN 314-434-5067**
- **DECC Huntsville**
  - **256-876-4180, DSN 746-4180**
  - HuntsvilleOPS@csd.disa.mil
- **DECC Mechanicsburg**
  - **717-605-7426 Opt. 4, DSN 430-7426**
  - **1-800-443-2448**
  - MEC-SD_Multiservice@csd.disa.mil
- **DECC Montgomery**
  - **866-227-4325, DSN 596-3472/3626**
  - **1-800-380-5575**
  - Mon-servicedesktickетrequest@csd.disa.mil
- **Montgomery HS OST (for MHS)**
  - **1-800-844-4145, DSN 596-6555**
  - Monmhsops@csd.disa.mil

- **DECC Ogden**
  - **866-419-3730, DSN 388-7901**
  - OgdenServiceDeskTriage@csd.disa.mil
- **DECC Oklahoma City**
  - **1-800-490-1643 Opt. 4, DSN 339-5600**
  - Okcservicedesk@csd.disa.mil
- **DECC Pacific**
  - **808-473-2020, DSN 473-2020**
- **DECC San Antonio**
  - **210-925-1923, DSN 945-1923**
  - SAT_OPS_ServiceDesk@csd.disa.mil
- **DECC St. Louis**
  - **314-260-0000 Opt. 4, DSN 490-0000**
  - SMChelp@csd.disa.mil
- **DECC Warner Robins**
  - **478-926-8026, DSN 468-8026**
  - AllWarnerRobins@csd.disa.mil
- **Theater Enterprise Computing Center (TECC) Bahrain**
  - **318-439-9325, DSN 439-9325**

13 APPENDIX A: ACRONYMS

The following acronyms are referenced throughout this document.

Acronym	Definition
ACC	Area Control Center
AS&W	Attack, Sensing, and Warning
ATAAPS	Automated Time Attendance and Production System
ATO	Authority to Operate
B2B	Business to Business
BAC	Business Availability Center
BEI	Background Environmental Information
BGP	Border Gateway Protocol
BES	BlackBerry Enterprise Server
C2	Command and Control
C&A	Certification and Accreditation
CAC	Common Access Card
CCRI	Command Cyber Readiness Inspection
CC/S/A	Combatant Commands, Military Services, and DoD Agencies
CE	Customer Edge
CM	Configuration Management
CND	Computer Network Defense
COCOM	Combatant Command
COIN	Community of Interest Network
COMSATCOM	Commercial Satellite Communications
CONOPS	Concept of Operations
CONUS	Continental United States
COOP	Continuity of Operations
CoS	Class of Service
CRM	Customer Relationship Management
CSD	Computing Services Directorate
CSS	Commercial Satellite Services
DAA	Designated Approving Authority

DGSC	DISB Global Support Center
DaaS	Database as a Service
DDOE	DISA Direct Order Entry
DECC	Defense Enterprise Computing Center
DFAS	Defense Finance and Accounting Service
DIA	Defense Intelligence Agency
DIACAP	DoD Information Assurance Certification and Accreditation Process
DIME	Deployment, Implementation, Maturization and Effectiveness
DISA	Defense Information Systems Agency
DISN	Defense Information Systems Network
DMS	Defense Messaging System
DMZ	Demilitarized Zone
DoD	Department of Defense
DoDD	Department of Defense Directive
DoDI	Department of Defense Instruction
DoDIIS	DoD Intelligence Information System
DSN	Defense Switched Network
DSA	Dynamic Spectrum Access
DSO	Defense Spectrum Organization
DVS-G	DISN Video Service – Global
DWCF	Defense Working Capital Fund
E3	Electromagnetic Environmental Effects
EL-CID	Equipment Location-Certification Information Database
eMASS	Enterprise Mission Assurance Support Service
EMC	Electromagnetic Compatibility
EMSS	Enhanced Mobile Satellite Services
EOB	Electronic Order of Battle
JEPS	Enterprise Portal Service
EW	Electronic Warfare
FMS	Foreign Military Sales
FRRS	Frequency Resource Record System
FSO	Field Security Operations
FTP	File Transport Protocol

FW	Firewall
GAL	Global Address List
GB	Gigabyte
GCDS	Global Content Delivery Service
GEMSIS	Global Electromagnetic Spectrum Information System
GETS	Government Emergency Telephone System
GEX	Global Exchange
GIG	Global Information Grid
GISMC	GIG Global Infrastructure Service Management Center
GMF	Government Master File
GRE	Generic Routing Encapsulation
GSSC	Global SATCOM Support Center
GSVS	Global Secure Voice System
GUI	Graphic User Interface
HERO	Hazards of Electromagnetic Radiation to Ordnance
HNCR	Host Nation Coordination Request
HP	Hewlett-Packard
HNSWDO	Host Nation Spectrum Worldwide Database Online
HVAC	Heating, Ventilating, and Air Conditioning
IA	Information Assurance
IARR	Information Assurance Readiness Review
IASE	Information Assurance Support Environment
IAVA	Information Assurance Vulnerability Alert
IC	Intelligence Community
IFL	Integrated Facility for Linux
IIS	Internet Information Services
IMS	Identity Management Solution
INMARSAT	International Maritime Satellite
IP	Internet Protocol
IRRT	Incident Response and Recovery Team
ISDN	Integrated Services Digital Network
IT	Information Technology
ITU	International Telecommunications Union

J2EE	Java 2 Enterprise Edition
JCSS	Joint Communication Simulation System
JETS	Joint Equipment Tactical and Space
JCSS	Joint Communication Simulation System
JOERAD	Joint Spectrum Center Ordnance Electromagnetic Environmental Effects Risk Assessment Database
JSC	Joint Spectrum Center
JSDR	Joint Spectrum Data Repository
JWICS	Joint Worldwide Intelligence Communications System
KPI	Key Performance Indicators
LAN	Local Area Network
LPAR	Logical Partition
M&S	Modeling and Simulation
MA	Multiple Access
MAC	Mission Assurance Category
MB	Megabyte
MCEP	Multiple Commercial Wireless Service
MIAP	Mainframe Internet Access Portal
MLPP	Multi-Level Precedence and Preemption
MLS	Multilevel Security
MQ	Message Queuing
MSP	Managed Service Provider
MSS	Mobile Satellite Service
NATO	North Atlantic Treaty Organization
NetOps	Network Operations
NIPRNet	Non-Secure Internet Protocol Routing Network
NMCC	National Military Command Center
NOC	Network Operating Center
NSA	National Security Agency
NSTS	National Secure Telephone System
NTIA	National Telecommunications and Information Administration
OCONUS	Outside the Continental United States
OE	Operating Environment

O&M	Operations and Maintenance
OPR	Office of Primary Responsibility
OS	Operating System
OS33	DSO Systems Engineering Branch
OS45	DSO JSC Electromagnetic Environmental Effects Division
OS48	DSO JSC Applied Engineering Division
OSD	Office of the Secretary of Defense
OWA	Outlook Web Access
PB Collo	Policy-Based Co-Location
PMO	Program Management Office
POC	Point of Contact
PPSM	Ports, Protocols and Services Management
PSTN	Public Switched Telephone Network
QoS	Quality of Service
RACE	Rapid Access Computing Environment
RDT&E	Research, Development, Test & Evaluation
RF	Radio Frequency
RFI	Radio Frequency Interference
RFP	Request for Proposal
RPO	Recovery Point Objective
RRC	Remote Recovery Combination
RSC	Regional Support Center
RSSC	Regional SATCOM Support Center
RTO	Recovery Time Objective
RUDICS	Router Unrestricted Digital Information Connectivity Solution
SA	System Administrator
SAAT	System Architecture, Analysis, and Testing
SAR	Synthetic Aperture Radar
SATCOM	Satellite Communications
SAV	Security Assistance Visit
SBD	Short Burst Data
SBU	Sensitive But Unclassified
SCI	Sensitive Compartmented Information

SCOM	Sytems Center Operations Manager
SCS	Spectrum Certification System
SES	Spectrum Enterprise Services
SFG	Secure File Gateway
SFTP	Secure File Transport Protocol
SIPRNet	Secure Internet Protocol Routing Network
SLA	Service Level Agreement
SME	Subject Matter Expert
SME-PED	Secure Mobile Environment – Portable Electronic Device
SMTP	Simple Mail Transfer Protocol
SOE	Standard Operating Environment
SOSC	Spectrum Operations Support Center
SS	Spectrum Supportability
SSEB	Source Selection Evaluation Board
SSH	Secure Shell
SSL	Secure Socket Layer
SSRA	Spectrum Supportability Risk Assessment
SST	Spectrum Technology Testbed Initiative (STTI) Simulation Toolkit
STE	Secure Terminal Equipment
STIG	Security Technical Implementation Guide
STTI	Spectrum Technology Testbed Initiative
SyNAPS	System Network Availability Performance Service
T&E	Test and Evaluation
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TS	Top Secret
TS/C	Top Secret/Collateral
TS/SCI	Top Secret/Sensitive Compartmented Information
UAS	Unmanned Aerial Systems
UEN	Ultra-High Frequency Emergency Network
UPS	Uninterruptible Power Supply
URL	Uniform Resource Locator
USCYBERCOM	United States Cyber Command

VCF	Videoconferencing Facilities
VoIP	Voice over Internet Protocol
VoSIP	Voice over Secure Internet Protocol
VMS	Vulnerability Management System
VPN	Virtual Private Network
VRF	Virtual Routing and Forwarding
VTC	Video Teleconferencing
WAN	Wide Area Network
WIN-T	Warfighter Information Network - Tactical

14 APPENDIX B: REFERENCES AND CITATIONS

- CJCS Instruction 6510.01F, February 2011, Information Assurance (IA) and Support to Computer Network Defense (CND) http://www.dtic.mil/cjcs_directives/cdata/unlimit/6510_01.pdf
- DoD 8570.01-M, December 2005, Information Assurance Workforce Improvement Program http://iase.disa.mil/eta/iawip/content_pages/policyref.html
- DoD Directive 5015.2, March 2000, DoD Records Management Program http://www.defense.gov/webmasters/policy/dodd50152p.pdf
- DoD Directive 8500.01E, October 2002, Information Assurance (IA) http://www.dtic.mil/whs/directives/corres/pdf/850001p.pdf
- DoD Financial Management Regulation 7000.14-R, April 2011 http://www.defenselink.mil/comptroller/fmr/
- DoD Financial Management Regulation 7000.14-R, Volume 11B, December 2010, Reimbursable Operations, Policy and Procedures – Working Capital Funds (WCF) http://www.defenselink.mil/comptroller/fmr/11b/index.html
- DoD Instruction 4000.19, August 1995, Interservice and Intragovernmental Support http://www.dtic.mil/whs/directives/corres/pdf/400019p.pdf
- DoD Instruction 5200.01, October 2008, DoD Information Security Program and Protection of Sensitive Compartmented Information http://www.dtic.mil/whs/directives/corres/pdf/520001p.pdf
- DoD Instruction 8500.2, February 2003, Information Assurance (IA) Implementation http://www.dtic.mil/whs/directives/corres/pdf/850002p.pdf
- DoD Instruction 8510.01, November 2007, DoD Information Assurance Certification and Accreditation Process (DIACAP) http://www.dtic.mil/whs/directives/corres/pdf/851001p.pdf
- NIST Special Publication 800-53, August 2009, Recommended Security Controls for Federal Information Systems and Organizations http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf
- OMB Circular A-130, February 1996, Management of Federal Information Resources http://www.whitehouse.gov/omb/circulars_a130

Document Source

- All DoD Issuances http://www.dtic.mil/whs/directives/
- All OMB Circulars http://www.whitehouse.gov/omb/circulars/#numerical

DEFENSE INFORMATION SYSTEMS AGENCY
A COMBAT SUPPORT AGENCY